

Remote Gateway 9150

Installation and Administration Guide

Product release 1.5

Standard 3.1

January 2005



Remote Gateway 9150

Installation and Administration Guide

Product release:	1.5
Publication number:	555-8421-215
Document release:	Standard 3.1
Date:	January 2005

Copyright © 2005 Nortel. All Rights Reserved

Printed in Canada

All information contained in this document is subject to change without notice. Nortel reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

*Nortel, the Nortel logo, the Globemark, Unified Networks, Meridian 1 PBX, Communication Server 1000 (CS 1000), and Communication Server 2100 (CS 2100) are trademarks of Nortel.

TelStrat is a registered trademark of TelStrat International, Ltd. Microsoft, MS-DOS, and Windows are trademarks of Microsoft Corporation.

FCC: Customer instructions

The Remote Gateway 9150 unit complies with Part 68 of the FCC rules. On the bottom side of the equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

The Remote Gateway 9150 unit uses the following standard connections and codes: USOC Code: RJ21X, Facility Interface Code: 02DU5-64, and Service Order Code: 6.0F.

The REN number shown on the label is used to determine the number of devices that can be connected to the telephone line. Excessive RENs on the telephone line can result in the devices not ringing in response to an incoming call. The sum of the RENs should not exceed five (5.0). To be certain of the number of devices that can be connected to a line, as determined by the total RENs, contact the local telephone company.

If the equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service might be required. However, if advance notice is not practical, the telephone company will notify you as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

No repairs can be performed by you. If you experience trouble with this equipment, please contact the following for repair and warranty information:

Nortel
Product Service Center
640 Massman Drive. Nashville, TN 31210
Phone: 1-800-466-7835

If the equipment is causing harm to the telephone network, the telephone company might request that you disconnect the equipment until the problem is resolved.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission, or corporation commission for information.

Industry Canada: Equipment attachment limitation

NOTICE: The Industry Canada Label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational, and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, you should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. You should be aware that compliance with the above conditions might not prevent degradation in service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, can give the telecommunications company cause to request you to disconnect the equipment.

You should ensure, for your own protection, that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution can be particularly important in rural areas.

Caution: You should not attempt to make such connections yourself, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface can consist of any combination of devices subject only to the requirements that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

Publication history

January 2005	This is the Standard 3.1 issue of the <i>Remote Gateway 9150 Installation and Administration Guide</i> for Remote Gateway 9100 Series product release 1.5.
July 2004	This is the Standard 3.0 issue of the <i>Remote Gateway 9150 Installation and Administration Guide</i> for Remote Gateway 9100 Series product release 1.5.
September 2001	This is the Standard 2.0 issue of the <i>Remote Gateway 9150 Installation and Administration Guide</i> for Remote Gateway 9100 Series product release 1.3.0. Support for Communication Server 2100 (CS 2100) has been added along with new and enhanced feature information that was formerly published in the <i>Remote Gateway 9100 Series and RLC Release Notes</i> .
March 2000	This is the Standard 1.0 issue of the <i>Remote Gateway 9150 Installation and Administration Guide</i> for Remote Gateway 9100 Series product release 1.0.

Contents

About this document	xvii
About this guide	xviii
<i>How to use this guide</i>	xviii
Product overview	xix
Skills you need	xx
<i>Nortel product knowledge</i>	xx
<i>Telecommunications experience</i>	xx
<i>Data networking knowledge</i>	xxi
Conventions used in this guide	xxii
<i>Precautionary messages</i>	xxii
<i>Instructions for selecting menu options</i>	xxiii
<i>Instructions for displaying property sheets</i>	xxiii
<i>PBX terminology</i>	xxiv
Related information products	xxv
<i>Printed documents</i>	xxv
<i>CD-ROM</i>	xxvi
1 Remote Gateway 9150 description	1
Product introduction	2
<i>Remote Gateway 9150 hardware description</i>	3
<i>Add-on modules description</i>	8
<i>Connection options</i>	10
Operational characteristics	12
<i>System security</i>	12
<i>Trunk connections</i>	13
<i>64K (56K) dynamic adaptation</i>	14
<i>Bandwidth allocation</i>	14
<i>Connection types</i>	14
<i>Minimum call duration timer</i>	14
<i>Idle timer</i>	15
<i>How the timers work to control ISDN costs</i>	15

How the Remote Gateway 9150 unit works	16
<i>Outgoing call process</i>	17
<i>Incoming call process</i>	17
<i>Bridge Port</i>	18
<i>Host controlled call mode</i>	18
<i>Locally controlled call mode</i>	18
<i>QoS Transitioning Technology</i>	19
<i>Call scenario 1: host-controlled—internal corporate call</i>	20
<i>Call scenario 2: host-controlled—external corporate call</i>	22
<i>Call scenario 3: locally controlled mode—local call</i>	24
Telephones	26
<i>Supported digital telephone sets</i>	26
<i>M2000 series (M3310, and M3820 European models) and</i> <i>M39xx series digital telephone set model and</i> <i>accessory compatibility</i>	29
<i>M39xx series digital telephone set accessory compatibility</i>	30
<i>Supported telephone modules</i>	30
<i>Computer telephony integration (CTI) applications</i>	31
<i>Automatic Call Distribution (ACD) applications</i>	32
<i>Voice over IP features</i>	32
<i>QoS Transitioning Technology</i>	34
<i>Port management</i>	35
<i>Station priority</i>	36
<i>Connection bandwidth</i>	37
<i>Local calling</i>	37
<i>Online/offline table</i>	40
<i>Other supported features</i>	41
<i>Communications system and software requirements</i>	42
<i>Supported Codecs</i>	42
Administration software	43
<i>Administration PC connection options</i>	43
<i>Remote Gateway 9100 Series Configuration Manager</i>	43
<i>Command line interface</i>	44

2	Planning for Remote Gateway 9150 unit installation	45
	Installation checklist	46
	Physical environment	50
	<i>Space</i>	50
	<i>Temperature and humidity</i>	51
	<i>Mounting options</i>	52
	<i>Connections</i>	52
	<i>Cables included with the Remote Gateway 9150 unit</i>	53
	<i>Cables you must supply yourself</i>	53
	Network considerations	55
	<i>IP addressing and routing</i>	55
	<i>QoS</i>	56
	<i>Numbering plans</i>	57
	<i>Call blocking</i>	57
	Administration PC	59
	<i>Connection options</i>	59
	<i>Windows PC requirements</i>	62
	<i>Optivity Telephony Manager and Configuration Manager</i>	63
	Trunk connection management	64
	<i>QoS Transitioning Technology</i>	64
	<i>Online/offline schedule</i>	64
	<i>Changing the online/offline mode</i>	65
	<i>Trunk bandwidth allocation</i>	65
	Station configuration	66
	<i>RLC settings</i>	66
	<i>Remote Gateway 9150 unit settings</i>	68
	Security	70
	<i>Toll fraud</i>	70
	<i>Data network security</i>	70
	<i>System configuration</i>	71
	Planning for future growth	72
	<i>Adding DSP modules</i>	72
	<i>Adding trunk interface modules</i>	73
	<i>Maximum configurations</i>	73
	Deployment options	75
	<i>Port and station assignment</i>	75
	<i>Implementing PSTN mode</i>	76
	<i>Implementing Voice over IP mode</i>	77
	<i>Implementing Remote Gateway 9150 units behind Network Address Translation (NAT) routers</i>	78
	<i>Implementing QoS Transitioning Technology</i>	79

Planning the configuration	81
<i>Data entry form completion sequence</i>	81
<i>Station assignments and configuration</i>	81
<i>ISDN BRI information</i>	82
<i>IP addresses</i>	83
<i>Connection link between the RLC and</i> <i>the Remote Gateway 9150 unit information</i>	83
<i>Online/offline schedule</i>	83
<i>Trunk configuration information</i>	84
<i>Numbering plan</i>	84

3 Installing the Remote Gateway 9150 unit 85

General safety	86
<i>Precautionary messages</i>	86
<i>Safety precautions</i>	87
Required installation tools	88
<i>Required tools for hardware installation</i>	88
<i>Required tools for software installation or upgrade</i>	88
Unpacking and inspecting the equipment	89
Removing and replacing the Remote Gateway 9150 unit cover	90
Installing trunk interface or DSP application modules	93
<i>Determining when to install trunk interface or</i> <i>DSP application modules</i>	93
<i>Determining where to install the modules</i>	94
<i>Installing trunk interface or DSP application modules</i>	96
<i>Removing trunk interface or DSP application modules</i>	96
Installing the Remote Gateway 9150 unit	98
<i>Choosing a suitable location</i>	98
<i>Installing the Remote Gateway 9150 unit on a desk</i>	99
<i>Installing the Remote Gateway 9150 unit on the wall</i>	100
<i>Installing the Remote Gateway 9150 unit in a rack</i>	103
Connecting the Remote Gateway 9150 unit	105
<i>Cables you must provide</i>	105
<i>Connector and pin-out reference</i>	106
<i>More information</i>	106
<i>Remote Gateway 9150 unit connection panel</i>	107
<i>Attaching the cables to Remote Gateway 9150 unit</i>	108
<i>Connecting the Remote Gateway 9150 unit to the network</i>	109
Powering up the Remote Gateway 9150 unit	111
<i>Power-up self-test</i>	111
<i>LED indicator test sequence</i>	112
Installing the Configuration Manager software	113

Using the Configuration Wizard to perform initial configuration	115
<i>What you can configure with the Configuration Wizard</i>	<i>115</i>
<i>Starting Configuration Manager</i>	<i>116</i>
<i>Establishing a serial connection</i>	<i>117</i>
<i>Performing configuration with the Configuration Wizard</i>	<i>119</i>
Testing the network connections	129
<i>Verifying telephone network connectivity</i>	<i>129</i>

4 Using Configuration Manager 133

What is Configuration Manager?	134
Starting and viewing Configuration Manager	135
Configuration Manager description	137
<i>Parts of the Configuration Manager screen</i>	<i>137</i>
<i>Menu Bar</i>	<i>137</i>
<i>System tree</i>	<i>138</i>
<i>Property sheets</i>	<i>139</i>
<i>Drop down boxes</i>	<i>139</i>
<i>Check boxes</i>	<i>140</i>
<i>Option buttons</i>	<i>140</i>
<i>Scroll boxes</i>	<i>141</i>
<i>Scroll bars</i>	<i>142</i>
<i>Command buttons</i>	<i>143</i>
Using online Help	144
Configuration files description	145
<i>Configuration Manager: File operations diagram</i>	<i>145</i>
<i>Types of files</i>	<i>146</i>
<i>Configuration Manager: File operations description</i>	<i>148</i>
Working with configuration files	153
<i>When to use the Configuration Manager file operations</i>	<i>153</i>
<i>Creating a configuration file on the PC</i>	<i>154</i>
<i>Opening a configuration file</i>	<i>154</i>
<i>Uploading a configuration to a unit</i>	<i>155</i>
<i>Downloading a configuration from a unit</i>	<i>155</i>
Selecting the device type for offline configuration	156
Logging on to a unit	157
<i>Connection types</i>	<i>157</i>
<i>Default logon ID and password</i>	<i>157</i>
<i>Connection history</i>	<i>157</i>
<i>Auto logoff</i>	<i>158</i>
<i>Logging on to a unit using the connection history</i>	<i>158</i>
<i>Logging on to a unit using Telnet</i>	<i>161</i>
<i>Logging on to a unit using the serial port</i>	<i>164</i>

Logging off of the unit	166
Using the Remote Connection command	167
Performing a system restart or shutdown	169
<i>When to perform a restart or shutdown</i>	169
Closing Configuration Manager	171
Uninstalling the Configuration Manager software	172

5 Configuring the Remote Gateway 9150 unit 173

9150 System configuration	174
<i>NLP</i>	175
<i>Emergency service programmability</i>	176
<i>Configuring the Remote Gateway 9150 system settings</i>	176
International tones support	186
<i>Configuring International Tones</i>	188
IP configuration	192
<i>Configuring the IP addresses</i>	193
<i>IP Configuration field descriptions</i>	193
<i>Prioritizing voice traffic over shared networks</i>	197
RLC connection configuration	198
<i>Configuring the RLC connection information</i>	199
<i>PSTN connection configuration</i>	199
<i>Security level configuration</i>	200
9150 port configuration	207
<i>Configuring stations</i>	208
<i>Bridge Ports</i>	214
<i>Analog port</i>	220
<i>Configuring a fax station</i>	221
<i>Configuring the fax port</i>	222
BRI configuration	225
<i>Remote Gateway 9150 ISDN BRI Interface information—</i> <i>for Norway and Sweden only</i>	226
<i>ISDN Line Type</i>	226
<i>Automatic TEIs (Terminal Endpoint Identifiers)</i>	227
<i>Entering the BRI settings</i>	227

Trunk group configuration	232
<i>Trunks</i>	233
<i>Primary trunk on the Remote Gateway 9150 unit</i>	233
<i>Trunk groups</i>	234
<i>Trunk access codes</i>	234
<i>ISDN configuration</i>	235
<i>European ISDN</i>	235
<i>National ISDN</i>	235
<i>Configuring trunk groups</i>	236
DSP configuration.	239
<i>Module identification</i>	240
<i>Device configuration</i>	240
<i>Configuring DSPs</i>	240
Auto upgrade configuration	243
<i>Configuring automatic upgrade</i>	244
Syslog configuration.	247
<i>Configuring syslog functionality</i>	248
Station configuration.	250
<i>Bridge Ports</i>	250
<i>Call processing capabilities and station settings</i>	251
<i>Call appearance keys</i>	253
<i>MCR keys increase DSP requirements</i>	254
<i>Private lines</i>	255
<i>Calling permissions and restrictions</i>	255
<i>ATA- and MCA-equipped stations and bandwidth requirements</i>	257

6 Using Remote Gateway 9150 stations 259

Modes of operation	260
<i>Host-controlled mode</i>	260
<i>Locally controlled mode</i>	261
<i>Relationship between host-controlled and locally controlled modes</i>	261
<i>Online mode</i>	262
<i>Offline mode</i>	262
<i>Why offline mode is important</i>	262
<i>What controls the online and offline modes</i>	263

Placing and receiving calls	264
<i>Receiving incoming calls</i>	<i>264</i>
<i>Methods for placing outgoing calls</i>	<i>265</i>
<i>Placing host-controlled calls</i>	<i>265</i>
<i>Placing outgoing locally controlled calls</i>	<i>266</i>
<i>Calling another station at your site</i>	<i>267</i>
Indicator updates.	268
<i>Host-controlled indicator updates</i>	<i>268</i>
<i>Locally controlled indicator updates</i>	<i>269</i>
Display messages	270
<i>Message descriptions</i>	<i>270</i>
Telephone features operation	273
<i>Emergency service calls.</i>	<i>273</i>
<i>Hold</i>	<i>274</i>
<i>Call Waiting</i>	<i>274</i>
<i>Call Transfer</i>	<i>275</i>
<i>Conference</i>	<i>276</i>
<i>Call Forward</i>	<i>276</i>
<i>Paging</i>	<i>276</i>
Going online and offline.	277
<i>Using the SPRE code to put all stations into online mode.</i>	<i>277</i>
<i>Using the SPRE code to put all stations into offline mode</i>	<i>277</i>
<i>Overriding an automatic offline event from the host PBX.</i>	<i>278</i>

7 Administration 279

Changing the administration password.	280
<i>Changing the Configuration Manager password</i>	<i>280</i>
<i>Changing the Remote Gateway 9150 unit password</i>	<i>281</i>
Creating a backup configuration file	282
<i>Storing backup configuration files.</i>	<i>282</i>
<i>Creating the backup file.</i>	<i>283</i>
Restoring the configuration	285
<i>Before you begin</i>	<i>285</i>
<i>Uploading a configuration file over the IP network</i>	<i>286</i>
Display logs	290
<i>Viewing display logs.</i>	<i>290</i>
<i>Printing the display logs to a file.</i>	<i>291</i>
<i>Changing the size of Remote Gateway 9150 unit logs.</i>	<i>292</i>
<i>Clearing logs</i>	<i>293</i>

Statistics screens	294
<i>Trunk Connection Statistics</i>	294
<i>Bandwidth Connection Statistics</i>	297
<i>Caller Info Statistics</i>	300
<i>Hardware Statistics</i>	303
<i>DSP Statistics</i>	307
<i>Ethernet Interface Statistics</i>	311
<i>BRI Information Statistics</i>	315
<i>Local Call Statistics</i>	318
<i>Remote Call Statistics</i>	320
<i>Device Information Statistics</i>	322
<i>ISDN Module Information Statistics</i>	325
<i>Network Statistics</i>	327
<i>PSTN Error Statistics</i>	332
Verifying the firmware and software version	335
<i>Verifying the software version</i>	335
<i>Verifying the firmware version</i>	336
<i>Determining the current firmware and software versions</i>	336
Obtaining the latest upgrade file	337
<i>Types of upgrades</i>	337
<i>Downloading the upgrade file</i>	337
Performing a firmware upgrade	338
<i>Manual firmware upgrade</i>	338
<i>When to perform a firmware upgrade</i>	339
<i>About firmware upgrades and configuration files</i>	339
<i>Before you begin</i>	339
<i>Upgrading the Remote Gateway 9150 unit firmware</i>	340
<i>Automatic or scheduled firmware upgrade</i>	342
<i>Self-contained firmware upgrade</i>	343
Performing a software upgrade	346
<i>Upgrading the Configuration Manager software</i>	346

8 Troubleshooting 347

Before you begin	348
<i>Identifying why a problem occurred</i>	348
Remote Gateway 9150 unit LED indicators	349
<i>What to do if the LEDs do not display correctly</i>	349
Digital telephone set	351
<i>Symptoms descriptions</i>	351
Device connectivity	356
<i>Symptom descriptions</i>	356

Software problems	360
<i>Symptom descriptions</i>	360
Using Configuration Manager PING	362
<i>Performing a Configuration Manager PING.</i>	362
<i>Unsuccessful PING options</i>	364
Syslog testing	365
<i>Performing Syslog testing</i>	365
Alarms and alerts	366
Responding to a catastrophic failure	367
<i>Inoperative hardware.</i>	367
Repair and warranty information	368
<i>Canada</i>	368
<i>United States</i>	368
<i>Europe</i>	369
<i>Asia/Pacific</i>	369
<i>CALA</i>	369
A Planning forms	371
Overview	372
<i>Network planning.</i>	372
<i>Remote Gateway 9150 forms</i>	372
<i>Data entry form completion sequence</i>	372
Completing the Remote Gateway 9150 forms	374
B Sample configuration files	389
Example of a network	390
<i>Sample configuration printouts</i>	390
<i>Configuration recommendation</i>	390
<i>Network diagram</i>	391
Voice port configuration on the Meridian 1 PBX	392
Data port configuration on the Meridian 1 PBX	394
RLC configuration	396
Remote Gateway 9150 unit configuration	400
C Pin-out tables for connections	403
TELCO 1 connector pin-out table	404
TELCO 2 connector pin-out table	406
Ethernet connector pin-out table	408
Admin (serial) connector pin-out table	409
Power connector pin-out table	410

D	Display log definitions	411
	Display logs	412
	Glossary	485
	Fields index	507
	Index	515

Preface

About this document

In this preface

About this guide	xviii
Product overview	xix
Skills you need	xx
Conventions used in this guide	xxii
Related information products	xxv

About this guide

The *Remote Gateway 9150 Installation and Administration Guide* (NTP 555-8421-215) is for telecom and data network managers and administrators who plan, install, and manage corporate telecommunications and data networks. This guide contains the following information:

- a detailed description of the Remote Gateway 9150 unit
- procedures necessary to properly install, configure, and manage the Remote Gateway 9150 unit at a location remote from the host PBX
- troubleshooting procedures for addressing possible problems

This guide assumes that you are familiar with the following:

- basic telecommunications terminology
- basic networking terminology
- PC terminology and operation (specifically, Windows 95, 98, NT Workstation 4.0, Millennium Edition (ME), 2000 Professional, XP [Professional and Home Edition])
- Nortel PBX terminology, functionality, and administration

How to use this guide

This guide provides step by step procedures for installing, configuring, and managing the Remote Gateway 9150 unit as a part of your Nortel remote services network. Review this guide before beginning Remote Gateway 9150 unit installation and configuration.

When you are ready to begin, follow the steps for planning, installing, and configuring your hardware in the order that they are presented in this guide. This helps you to achieve a successful, trouble-free installation.

Product overview

The Remote Gateway 9150 unit provides full-featured host PBX services to as many as 32 users located in your office.

The Remote Gateway 9150 solution consists of the following components:

- **Reach Line Card (RLC)**
The RLC is installed in the PBX at the host location and relays voice and signaling information from the digital telephones connected at the Remote Gateway 9150 site to the PBX at the host site.
- **Remote Gateway 9150 unit**
The Remote Gateway 9150 unit is installed in your office. It relays voice and signaling information between the digital telephones in your office to the PBX at the host location.
- **10BaseT Ethernet and ISDN Basic Rate Interface (BRI) connections**
These connections provide the voice and data connections between the Remote Gateway 9150 unit and the host PBX.
- **ISDN BRI trunk interface modules are supported for the following:**
 - U interface
 - S/T interface
- **optional Digital Signal Processor (DSP) application modules**
You can add these modules to increase the system's voice processing capacity.

The Remote Gateway 9150 unit uses the Voice over IP technology to route voice conversation and telephone set control signals between your office and the host PBX over your existing IP data network.

The Remote Gateway 9150 unit can also use the PSTN to route calls if:

- **the voice Quality of Service (QoS) degrades below predefined thresholds**
In this case, Nortel's patented QoS Transitioning Technology automatically transitions calls to the PSTN when the voice QoS degrades. Calls transition back to the IP network when the QoS returns to normal.
- **you are not yet ready to use the IP network to route voice calls**
You can configure the Remote Gateway 9150 unit to use only the PSTN, and implement the IP network functionality when you are ready.

Skills you need

Knowledge of, or experience with, the following concepts as appropriate to your network is helpful when administering the Remote Gateway 9150 unit:

- Microsoft Windows
- software installation
- network configuration

Nortel product knowledge

Knowledge of, or experience with, the following Nortel products and concepts:

- basic administration of a Meridian 1, Communication Server 1000 (CS 1000), or Communication Server 2100 (CS 2100) PBX (telephone set and XDLC configuration)
- characteristics and principles of XDLC operation
- PBX data calls
- Meridian digital telephones

Telecommunications experience

Knowledge of, or experience with, the following aspects of telecommunications:

- Extended Digital Line Cards (XDLCs) and how they work
- configuring voice and data ports
- configuring ISDN BRI, PRI (or other types of trunks)
- establishing telephone connections

Data networking knowledge

Knowledge of, or experience with, the following aspects of data networking:

- data link (Layer 2 of the OSI model)
 - IP protocol
 - routing
- network (Layer 3 of the OSI model)
 - addressing
 - traffic analysis and provisioning
 - configuration
- Voice over IP concepts

Conventions used in this guide

This section describes the conventions used in this guide.

Precautionary messages

Note: A “Note” describes the secondary results of procedures or commands, or special conditions that require you to use a procedure or command.

ATTENTION! _____
Provides information essential to the completion of a task.



CAUTION

Risk of data loss or equipment damage

Cautions you against unsafe practices or potential hazards, such as equipment damage, service interruption, or loss of data.



WARNING

Risk of minor personal injury

Warns you of a potentially hazardous situation that can result in minor or moderate injury.



DANGER

Risk of electric shock

Alerts you to an immediate hazard that can result in death or serious injury through high voltage or electric shock.

Instructions for selecting menu options

To simplify the instructions for selecting menu options, this guide abbreviates the selection path. For example, if you must choose Over IP from the PSTN Connectivity menu, under the Tests menu, this guide uses the following style:

From the menu, choose Tests → PSTN Connectivity → Over IP.

Instructions for displaying property sheets

To simplify the procedures for accessing property sheets throughout this guide, the instructions for displaying a particular property sheet are summarized in a “Getting there” statement.

The procedure for displaying the screen that you need depends on if you are:

- performing an online configuration (connected to a node by serial port or Telnet)
- performing an offline configuration (not connected to a node)

Example

Getting there 9150 → Configuration Manager → IP Configuration

The long instruction for this example is as follows:

- 1 Do the following:

IF	THEN
you are performing an offline configuration,	select the device type as described in “Selecting the device type for offline configuration” on page 156.
you are performing an online configuration,	connect to, and then log on to the node as described in “Logging on to a unit” on page 157.

- 2 In the left pane, click on the plus sign (+) beside Configuration Manager to expand the node list.
- 3 Click on **IP Configuration**.

Result: The IP Configuration property sheet for the Remote Gateway 9150 unit displays in the right pane.

PBX terminology

Throughout this guide, the term “host PBX” refers to any of the following Nortel PBX platforms:

- Meridian 1 PBX
- CS 1000
- CS 2100

Related information products

This section lists sources for additional information related to the Remote Gateway 9150 unit. You can order printed documentation and the CD-ROM from your Nortel distributor.

You can also download the documentation in Portable Document Format (PDF) from the Nortel website. To locate these documents, click on the **Technical Documentation** link at the following website:

www.nortel.com

Note: The information available on the website may supersede the information provided on the CD-ROM.

For further details, refer to *Remote Gateway 9100 Series and RLC Release Notes* (NTP 555-8421-102).

Printed documents

The following documents provide additional information on the RLC and other elements of a Remote Gateway 9100 Series system:

Remote Gateway 9100 Series Network Engineering Guidelines **(NTP 555-8421-103)**

The *Remote Gateway 9100 Series Network Engineering Guidelines*, written for the installer/administrator, describe how a Remote Gateway 9100 Series system integrates with existing telecommunications and data networks. This document helps you to ensure that your networks are prepared for 9150.

Remote Gateway 9100 Series and RLC Release Notes **(NTP 555-8421-102)**

The *Remote Gateway 9100 Series and RLC Release Notes*, written for the installer/administrator, describe the features and known problems for the different elements of a 9150 system. This document contains information pertaining to the Reach Line Card (RLC), the Remote Gateway 9150 unit, Remote Gateway 911x series units, and Digital Telephone IP Adapter units.

***Reach Line Card Installation and Administration Guide
(NTP 555-8421-210)***

The *Reach Line Card Installation and Administration Guide*, written for the installer/administrator, describes how to install, configure, and manage the Reach Line Card on the host PBX.

***Remote Gateway 911x Series Installation and Administration Guide
(NTP 555-8421-220)***

The *Remote Gateway 911x Series Installation and Administration Guide*, written for the installer/administrator, describes how to install, configure, and manage Remote Gateway 911x series units.

***Digital Telephone IP Adapter Installation and Administration Guide
(NTP 555-8421-211)***

The *Digital Telephone IP Adapter Installation and Administration Guide*, written for the installer/administrator, describes how to install, configure, and manage Digital Telephone IP Adapter units.

Installer's Notes

The following Installer's Notes are quick reference documents that are provided with the component discussed in the document:

- Reach Line Card Installer's Notes
- Remote Gateway 9150 and RLC DSP Application Module Installer's Notes
- Remote Gateway 9150 Trunk Interface Module Installer's Notes

CD-ROM

A Remote Gateway 9100 Series Product CD-ROM is available containing the documentation in Portable Document Format (PDF), firmware, and Remote Gateway 9100 Series Configuration Manager software.

Chapter 1

Remote Gateway 9150 description

In this chapter

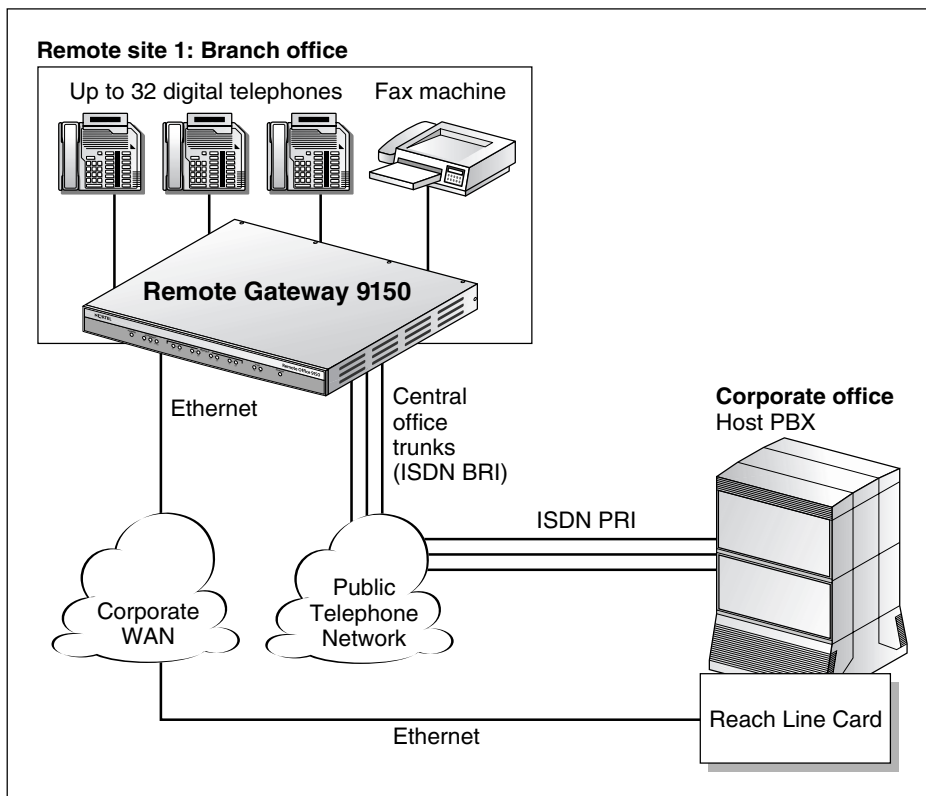
Product introduction	2
Operational characteristics	12
How the Remote Gateway 9150 unit works	16
Telephones	26
Administration software	43

Product introduction

The Remote Gateway 9150 unit installed in your office provides PBX functionality for up to 32 digital telephones. Voice and signaling information between the digital telephones connected at your office and the RLC installed on the PBX at the host location is relayed over one or both of the following:

- IP network
- PSTN

The illustration below shows the connection between a Remote Gateway 9150 unit and an RLC.



G101391

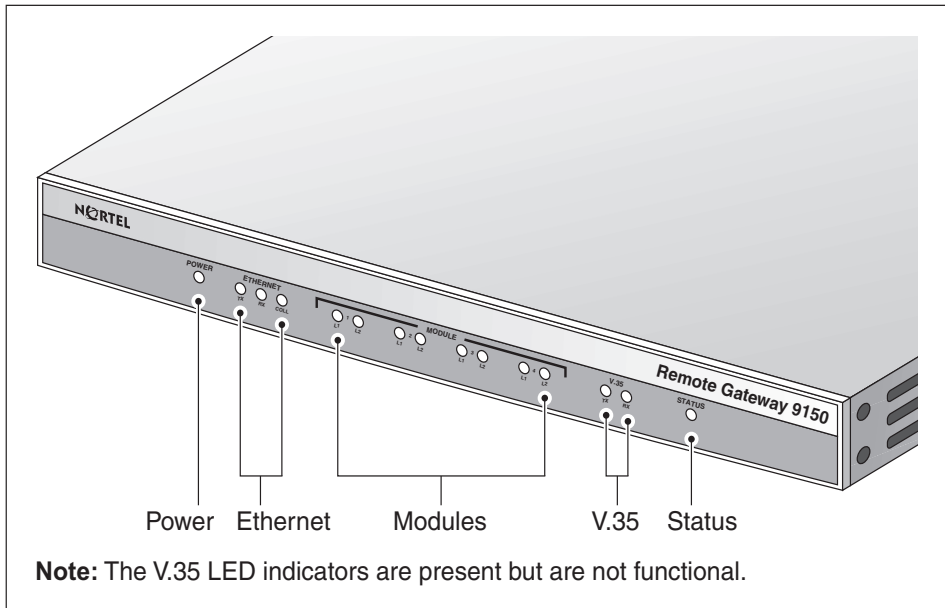
Note: Nortel does not support a Remote Gateway 9100 Series system as a free-standing key system.

Remote Gateway 9150 hardware description

The Remote Gateway 9150 unit is installed in your office and can be mounted on a desk, in a rack, or on the wall. This section describes the LED indicator displays, power supply, cables, and connectors for the unit.

LED indicators on the Remote Gateway 9150 unit

The following diagram shows the LED indicators on the front panel of the Remote Gateway 9150 unit.



G101402

The operational status of the Remote Gateway 9150 unit is indicated by these LEDs as described in the following table.

LED indicator type	LED indicator name	Description
Power	On	When lit, this LED indicator signifies that power is present.
Ethernet	TX	When flashing, this LED indicator signifies that data is being transmitted by the Remote Gateway 9150 unit over the Ethernet network.
	RX	When flashing, this LED indicator signifies that data is being presented to the Remote Gateway 9150 unit over the Ethernet network.
	COLL	When flashing, this LED indicator signifies that a collision has occurred on the Ethernet network.
Module	L1 and L2	L1 LED indicator: <ul style="list-style-type: none"> ■ not lit: there is no D-channel activity ■ flashing: the D-channel is active but the B-channel is not active ■ lit solid: both the D- and B-channels are active L2 LED indicator: <ul style="list-style-type: none"> ■ not lit: the B-channel is not active ■ lit: the B-channel is active
V.35	TX	For future use.
	RX	For future use.
Boot status	Status	Indicates the condition of the Remote Gateway 9150 unit. This LED indicator stays lit when the power on self-test is successful. If it goes out, there is a problem.

Collisions

Half-duplex Ethernet connections only allow their nodes to either send or receive packets at any given time. Collisions occur when two nodes on a half-duplex Ethernet connection attempt to transmit information simultaneously. Before transmitting, the Network Interface Card (commonly referred to as the NIC card) monitors the line, or listens, for transmissions. A NIC card listens to the line for the amount of time that it takes to transfer a minimum-sized packet the maximum length of the cable. If the NIC card senses no transmission from the destination node, it proceeds with its own transmission.

If a NIC card detects a collision, it waits for a period of time determined by the back-off algorithm, then re-transmits the packet. Ethernet nodes keep track of how many times they must re-transmit a packet with a maximum collision re-try counter. In previous versions of Remote Gateway 9100 Series software, the maximum collision re-try counter had a limit of 15. After 16 unsuccessful attempts to transmit a packet (the original attempt plus 15 re-tries) the Remote Gateway 9100 Series unit dropped the packet. In an effort to decrease delay and improve QoS, the limit of the maximum collision re-try counter is now eight. After nine unsuccessful attempts to transmit a packet (the original attempt plus eight re-tries) the Remote Gateway 9100 Series unit drops the packet and begins attempting to transmit the next packet.

Note: Since Ethernet traffic has a nominal speed of 10 Mbps, the flashing Ethernet COLL, TX, RX LED indicators are cosmetic. They do not reflect real-time traffic patterns or packets.

Connectors

The following connections are made from the rear panel of the Remote Gateway 9150 unit to the telephone and data networks:

- Two 25-pair connectors (labeled TELCO 1 and TELCO 2) provide tip and ring connections to user stations (telephones) and central office trunks (ISDN BRI).

These connections provide the interface to the telephone network and the Public Switched Telephone Network (PSTN).

- An RJ-45 connector (labeled ETHERNET) provides a 10BaseT Ethernet connection.

This connection provides the ability to pass both voice and data traffic over the existing Ethernet network.

- A DB-9 connector (labeled ADMIN) provides an RS-232 serial port connection.
You can use this serial port connection to configure a Remote Gateway 9150 unit that is directly connected to a PC.

Refer to Chapter 2, “Planning for Remote Gateway 9150 unit installation,” for a detailed description of cables and connectors.

Mounting options

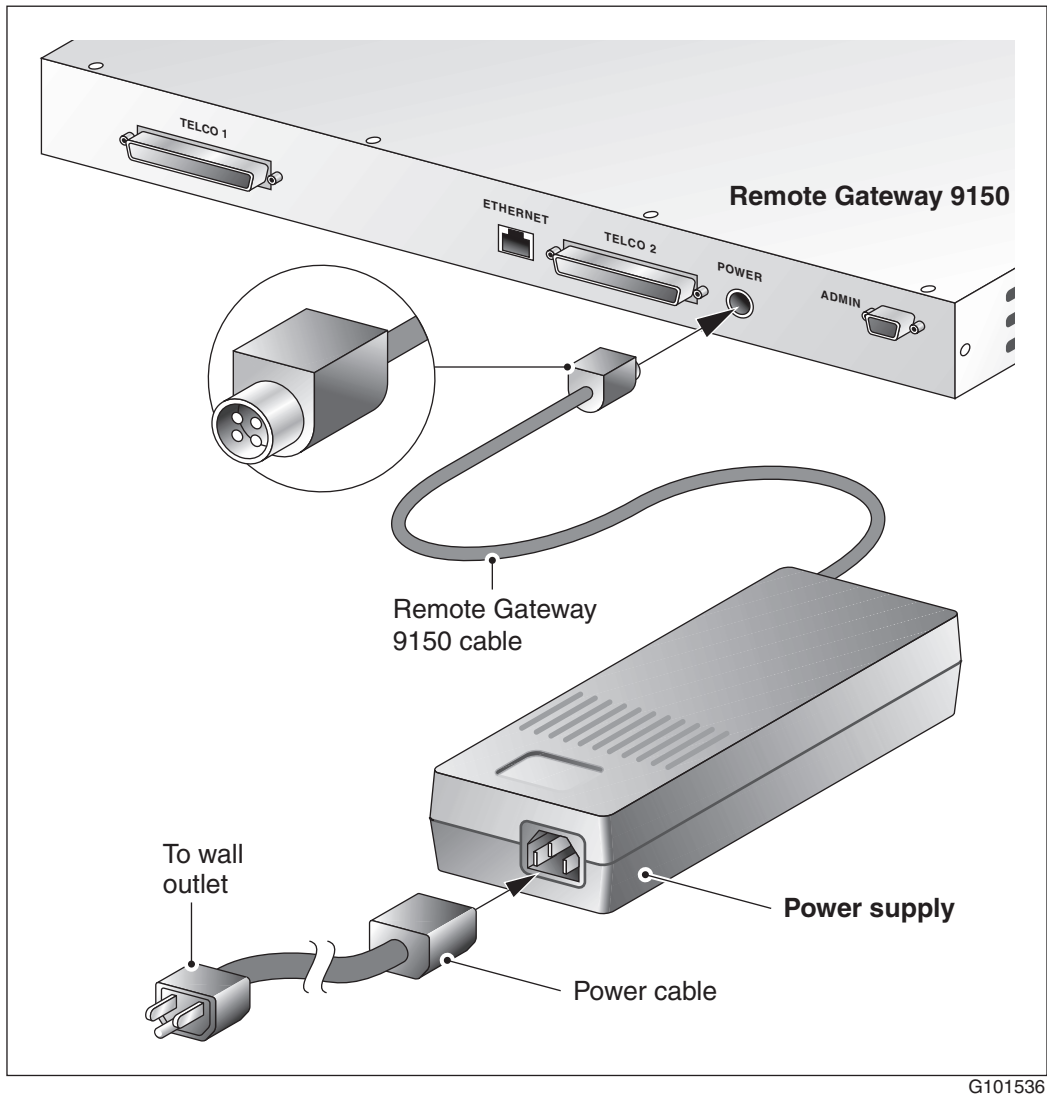
The Remote Gateway 9150 unit can be mounted on a desk, in a rack, or on the wall.

Universal power supply

The Remote Gateway 9150 unit includes an auto-sensing 110/220 V power supply that is compatible with commercially available UPS systems. Refer to the diagram on page 7.

Note: If you want to connect the Remote Gateway 9150 unit to a UPS, ensure that the UPS has a minimum rating of 100 Watts.

Remote Gateway 9150 power supply



Add-on modules description

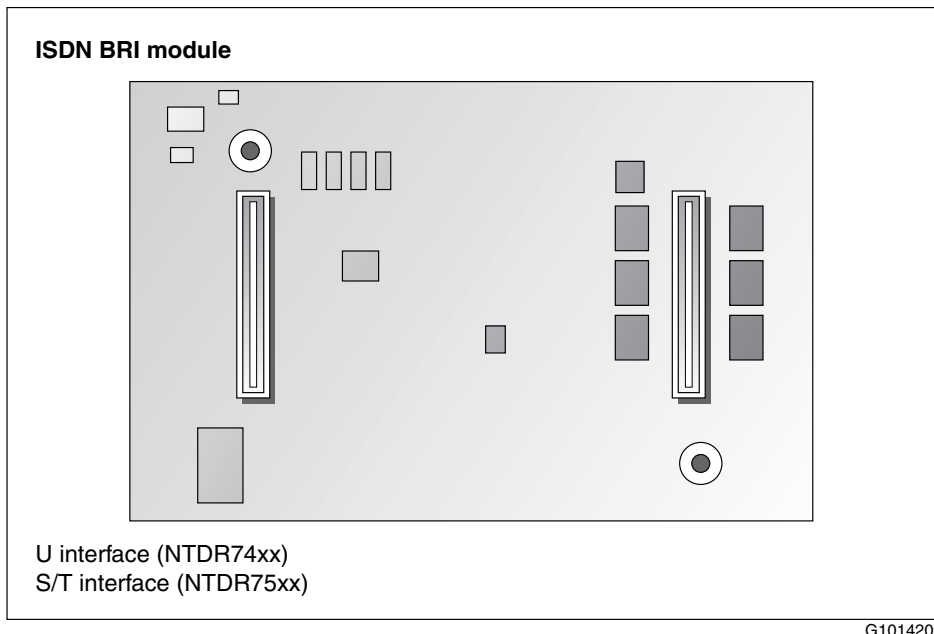
The Remote Gateway 9150 unit can support trunk interface modules, such as ISDN BRI U or S/T interfaces, and up to three DSP application modules.

Optional trunk interface modules

Trunk interface modules route calls over the PSTN. The number of modules you must install depends on the number of simultaneous calls you want to process in host-controlled or locally controlled mode.

Note: To determine how many trunk interface modules you need for your calling requirements, use the “Remote Gateway 9150 System expansion worksheet” on page 385.

The Remote Gateway 9150 unit can support up to four U or S/T ISDN BRI interfaces. Each module supports one ISDN BRI line (with two B-channels) from the local telephone service provider. Refer to the following illustration for an example of an ISDN BRI module:



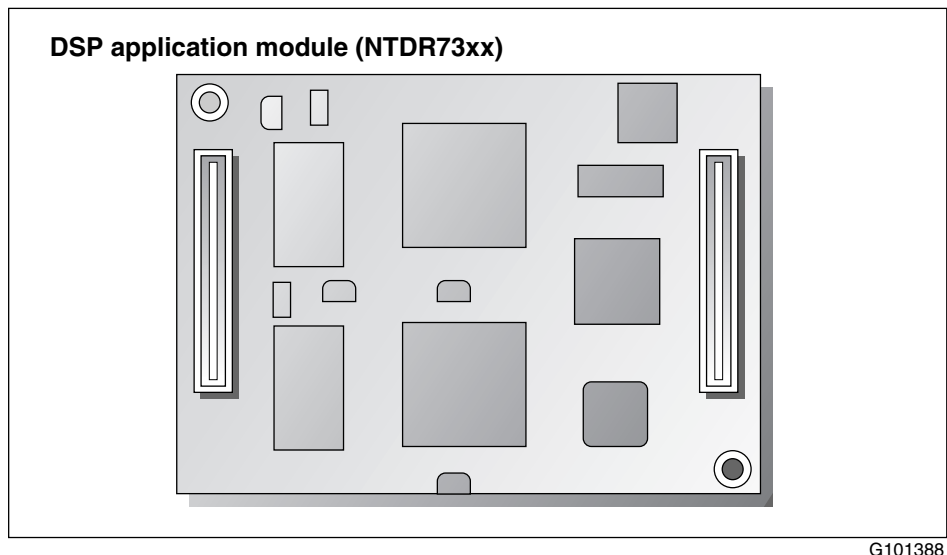
Note: Initially, the Remote Gateway 9150 unit ships with no ISDN BRI modules installed.

Optional DSP application modules

DSPs convert voice and fax into digital data for transport over the IP network and PSTN. Initially, the Remote Gateway 9150 unit ships with the ability to support up to eight simultaneous calls through a DSP that is built into the Remote Gateway 9150 unit's motherboard. To add support for up to 32 simultaneous calls, you must install DSP application modules. Up to three DSP application modules are supported. Each module provides up to eight more simultaneous calls.

Note: To determine how many DSP application modules you need for your calling requirements, use the "Remote Gateway 9150 System expansion worksheet" on page 385.

In addition, you can configure the Remote Gateway 9150 unit for blocking with only enough modules to support the maximum number of simultaneous calls. For example, a Remote Gateway 9150 unit that is equipped with a single DSP application module supports 16 simultaneous calls, for a ratio of 2 to 1 blocking. Refer to the following illustration for an example of a DSP application module:



Note: For more details, refer to "Planning for future growth" on page 72.

Connection options

Communications between the Remote Gateway 9150 unit in your office and the host PBX take place using 10BaseT Ethernet or ISDN BRI connections, or both. This section provides a description of each of these connections.

10BaseT Ethernet interface

Voice over IP technology is used to carry voice conversation and telephone set control signals over your IP network to the host PBX. The voice data is forwarded as UDP/IP packets, and the signaling data is forwarded as TCP/IP packets.

Note: The Remote Gateway 9150 unit, vintages AC, BC, CC, and earlier use a half-duplex 10BaseT Ethernet connection. Vintages AD, BD, CD and later default to a half-duplex 10BaseT Ethernet connection. You can configure a full-duplex 10BaseT Ethernet connection on units of these vintages through Configuration Manager. When you configure a full-duplex 10BaseT Ethernet connection, the Remote Gateway 9150 unit's Ethernet collision LED remains on solid (constantly lit). In addition, when you enable full-duplex Ethernet, you must also set the corresponding port on the connected switch to 10 FULL Duplex. Remote Gateway 9100 Series products do not support Auto negotiation of the Ethernet interface.

ISDN BRI lines to PSTN

The PSTN provides a cost-effective alternative to leased lines. You can use ISDN BRI lines at the Remote Gateway 9150 site to place local calls without involving the host PBX. You can also choose to use the ISDN BRI lines instead of the IP network to route calls through the host PBX.

To use ISDN BRI lines, you must install trunk interface modules. The Remote Gateway 9150 unit can support up to four U or S/T ISDN BRI trunk interface modules. (Refer to “Add-on modules description” on page 8.)

Quality of Service (QoS) Transitioning Technology

If both the IP network and ISDN BRI lines are used, you can use the QoS Transitioning Technology to re-route calls from the IP network to the PSTN when the QoS on the IP network degrades. When the QoS returns to normal, the QoS Transitioning Technology automatically moves the calls back to the IP network.

The Remote Gateway 9150 unit monitors the QoS on the IP network. If the QoS falls below pre-programmed acceptable thresholds, calls are dynamically and transparently switched to the ISDN BRI lines. Refer to “QoS Transitioning Technology” on page 34 for additional details.

Analog port for fax machines

The Remote Gateway 9150 unit has one analog port that you can use as a fax connection. Refer to “Fax support” on page 41 for more detailed information.

ATTENTION!

You cannot transfer a call on a telephone set connected to the analog port of a Remote Gateway 9150 unit. Remote Gateway 9100 Series does not support Switch Hook flash.

Operational characteristics

This section provides details on how the Remote Gateway 9150 unit functions.

System security

This section describes the security levels that are supported for controlling access from the Remote Gateway 9150 unit to the RLC on the host PBX.

- No security

When no security measures are used, the RLC accepts all incoming calls from the Remote Gateway 9150 site.

Use this level with caution as it can be prone to unauthorized use. For example, a user in your site could accidentally, or intentionally, enter a trunk number for another site and place long distance phone calls through this connection.

- Caller Identification (ID)

When Caller ID is used, and the PSTN routes the call, the RLC identifies the Remote Gateway 9150 unit's calling line identification (CLID). If the CLID matches the remote number configured on the port assigned to the Remote Gateway 9150 unit, access is granted. If the incoming call's CLID does not match, access is denied.

Note: Caller ID authentication cannot be performed over the IP network.

- Provision ID

You can use Provision Identification (ID) authentication over the IP network or PSTN. When you choose Provision ID, the Remote Gateway 9150 unit sends its 10-digit security identifier (password) for each connection request. The RLC compares the security identifier with the one configured on the RLC port where the Remote Gateway 9150 unit is assigned. If the security identifiers match, access is granted.

If the security identifiers do not match, then an event is recorded in the Remote Gateway 9150 unit system log (you can view the system log in Configuration Manager). The telephone that was used to place the call displays a message indicating that communications with the host PBX are down.

You must configure two security identifier passwords on the Remote Gateway 9150 unit:

- inbound security identifier: This is the RLC's security identifier. It is presented on incoming calls.
- outbound security identifier: This is the Remote Gateway 9150 unit's security identifier. It is presented to the RLC on outgoing calls.

You must configure the same security identifiers in reverse on this Remote Gateway 9150 unit's RLC port.

Trunk connections

The Remote Gateway 9150 unit supports the following digital trunk connections:

- ISDN BRI from the Remote Gateway 9150 unit to the PSTN
- ISDN PRI from the PSTN to the RLC at the host site

Multiple Subscriber Numbering (MSN)

Remote Gateway 9100 Series supports MSN. If the Central Office provides each B-channel with a unique DN, then the first B-channel that you configure defines the number for both B-channels.

Remote Gateway 9100 Series requires the ISDN numbers to be unique per module for PSTN connections between the RLC and Remote Gateway 9150 unit.

Do not configure B-channels as Local and Remote if MSN is disabled.

For Remote Gateway 9150 units with multiple BRI modules:

- Configure a maximum of one BRI module as Remote Only if PSTN connections are required.
- Configure all other BRI modules as Local only.

For Remote Gateway 9150 units with just one BRI module the BRI module can be configured as Local only or Remote only. If local ISDN calls and remote calls over PSTN are required, then MSN must be enabled.

64K (56K) dynamic adaptation

With some carriers, 64K calls routed over a 56K PSTN infrastructure may cause errors. The dynamic adaptation feature allows the Remote Gateway 9150 unit and the RLC to dynamically detect the limitation of the bandwidth. The call is then downgraded from 64K to 56K.

Bandwidth allocation

The RLC automatically allocates trunk bandwidth to the Remote Gateway 9150 connection as needed. For example, as calls are initiated and bandwidth requirements increase, additional trunk connections are established. Likewise, as calls terminate and bandwidth requirements drop, connections to idle trunks are terminated.

Connection types

The Remote Gateway 9150 connection to the RLC can be defined on the RLC as permanent or on demand. A permanent connection means that the ISDN connection to the host PBX always remains open. An on demand connection means that the ISDN connection is established only when a connection with the host PBX is required.

If the connection is defined as demand, then you can configure minimum call duration and idle timers on the RLC to help reduce call charges.

Minimum call duration timer

Most ISDN tariffs specify minimum charges incurred when you open the line, regardless of the call duration. This charge is the minimum call charge listed on long distance telephone bills.

The minimum call duration timer is used in PSTN mode only and specifies the minimum length of time that each PSTN call to the host PBX remains active, regardless of telephone activity or inactivity. Configure the timer on the RLC to drop inactive connections just before an additional charge period is incurred. For example, if the timer is set to 59 seconds and your call lasts only 20 seconds, the ISDN connection drops when the timer reaches 59 seconds.

If another call is made to the host PBX before the timer expires, the timer is reset. The timer tracks the current call.

Idle timer

The idle timer identifies the maximum length of time that an ISDN connection remains idle before Remote Gateway 9100 Series closes it. Idle means that a voice connection exists but is not active, and buttons are not being pressed on digital telephones.

For example, if the idle timer is set on the RLC to 60 seconds, the ISDN call remains open for 60 seconds after you hang up. If you or someone else dials another number before 60 seconds have passed, another ISDN connection is not opened.

How the timers work to control ISDN costs

The minimum call duration and idle timers work together to control ISDN charges. The following examples describe what happens when the minimum call duration timer is set to 59 seconds and the idle timer is set to 60 seconds.

Example 1

If the call lasts for 20 seconds and no other calls are made, the ISDN connection drops when the minimum call duration timer reaches 59 seconds. The minimum call duration timer expires before the idle timer.

Example 2

If the call lasts for 65 seconds and no other calls are made, the ISDN connection drops after another 60 seconds has passed without activity. Since the ISDN call exceeded 59 seconds, the minimum call duration timer no longer applies. The idle timer is used, in this case, to prevent further ISDN charges.

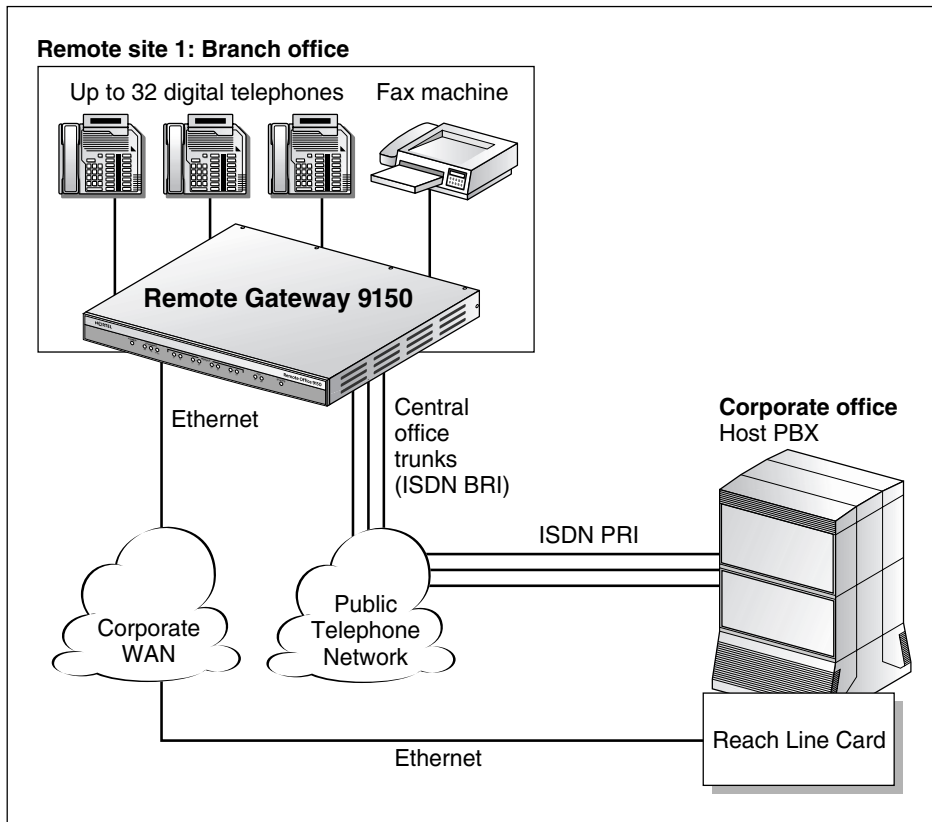
How the Remote Gateway 9150 unit works

There are two major components to the Remote Gateway 9150 product:

- the Remote Gateway 9150 unit located in your office
- the RLC located on the PBX at the host site

These two components, along with the connection options described on page 10, extend the host PBX services to users in your office.

The following diagram shows a RLC and Remote Gateway 9150 network:



Outgoing call process

To place outgoing calls, users can either pick up the handset on the telephone or press a line appearance key. There are two types of line appearance keys:

- host call appearance key
Use this key to place a call through the host PBX.
- local call appearance keys
Use these keys to place calls to other stations in your office, or to place and receive calls through the local PSTN. You can define up to two local call appearance keys on each digital telephone.

For a detailed description of the outgoing call process, refer to the sample illustrations beginning on page 20.

Incoming call process

When a user places a call through the host PBX to a user at the Remote Gateway 9150 site, a connection is made from the RLC to the Remote Gateway 9150 unit and the host PBX completes the call. If a connection cannot be established, then the call rings until it is forwarded to voice mail by the host PBX. Refer to Chapter 6, “Using Remote Gateway 9150 stations,” for a more detailed description of the incoming call process.

When someone places a call through the PSTN to a user at the Remote Gateway 9150 site, a connection is made from the central office to the Remote Gateway 9150 unit. The number that outside callers dial is the number assigned by the ISDN service provider to the ISDN BRI B-channel carrying the incoming call.

You can configure an unanswered incoming local call to Call Forward to a DN on the host PBX. The Bridge Port connects the call to the host PBX and it can then transfer to voicemail.

Bridge Port

A Bridge Port is a proxy port that represents a local or inbound PSTN call to the host PBX. When a local incoming call on a Remote Gateway 9150 unit needs PBX services, the Bridge Port obtains a PBX presence on behalf of the local call.

Bridge Ports can represent the following types of local calls:

- Call Forward: A Local and Remote call made to another Local and Remote telephone uses Call Forward to connect to a third telephone on the PBX.
- Call Transfer: A Local call to a Local and Remote telephone uses Call Transfer to connect to a local trunk or a host-based set.
- Conference: A Remote call to a host telephone can connect to trunk call(s), or if you are on a call to a local trunk, you can connect to host telephone(s) to create three-or-more-party telephone calls.

To configure Remote Gateway 9150 Bridge Ports refer to page 250.

Host controlled call mode

When a user places a call to someone at the host site, or when someone from the host site calls the Remote Gateway 9150 site, the call is in host-controlled call mode. Calls in host-controlled mode are routed through the host PBX. Refer to the sample illustrations on pages 20 and 22.

Locally controlled call mode

When a user places a call from a local call appearance key, or the call is to another telephone at the Remote Gateway 9150 site, the call is in locally controlled mode. Calls that are initiated from the local call appearance key are routed through the local PSTN. Calls to other extensions in the Remote Gateway 9150 site are routed only through the Remote Gateway 9150 unit.

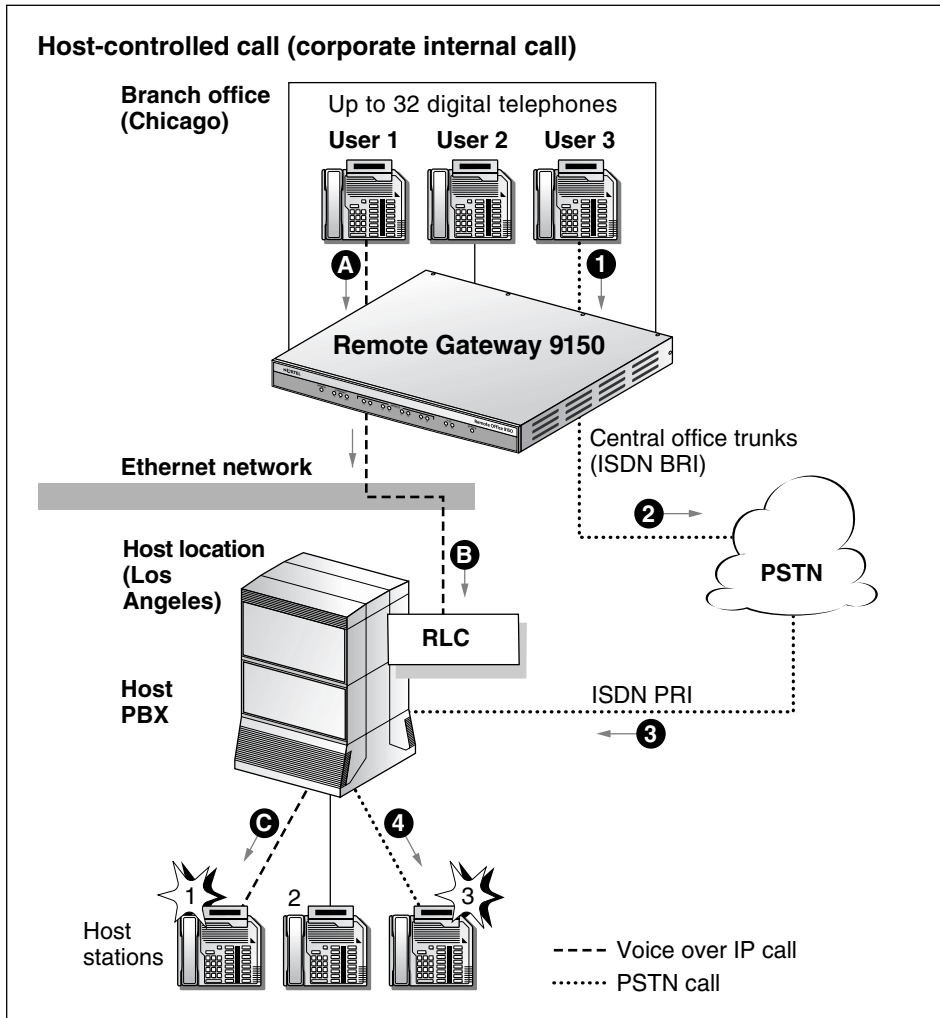
The host PBX is not involved in locally controlled mode calls. Refer to the sample illustration on page 24.

QoS Transitioning Technology

If the QoS on the IP network falls below a predefined threshold, you can configure the Remote Gateway 9150 unit to automatically route voice traffic away from the IP network connection to the PSTN connection. Refer to “QoS Transitioning Technology” on page 34 for a detailed description.

Call scenario 1: host-controlled—internal corporate call

The following diagram shows how a call is routed when making a host-controlled call to the corporate office.



G101392

The network that is used to route the host-controlled call is transparent to the user, and the dialing requirement is the same for both. Calls work the same way in reverse, from host PBX site to the Remote Gateway 9150 site.

Voice over IP network call

- 1 User 1 presses the host call appearance key.

Result: User 1 hears a dial tone. This indicates that the connection to the RLC over the IP network was successful.

- 2 User 1 dials a telephone number (such as the extension number of host station 1).

Result: The dialed digits are sent by the Remote Gateway 9150 unit as packets across the Ethernet network. The RLC converts the packets to the format required by the PBX. The PBX then converts the data to voice and routes the call to host station 1.

PSTN call

- 1 User 3 presses the host call appearance key.

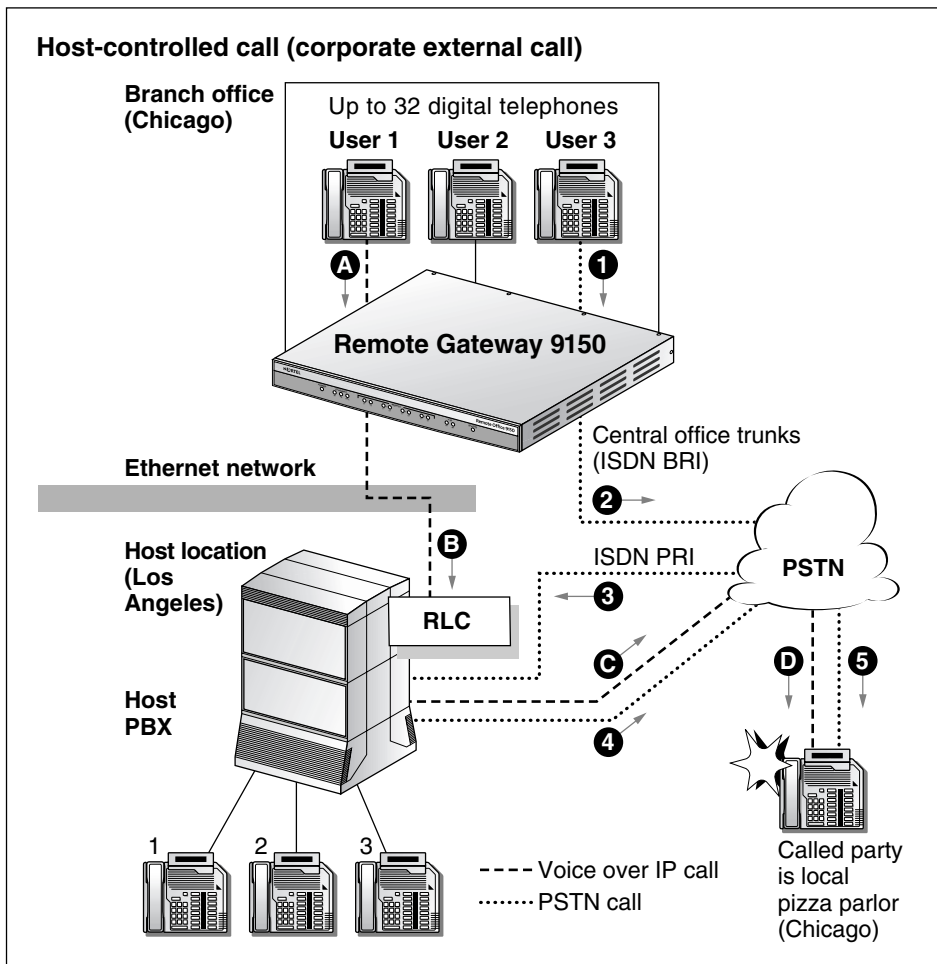
Result: User 3 hears a dial tone. This indicates that the connection to the RLC over the PSTN was successful.

- 2 User 3 dials the telephone number (such as the extension number of host station 3).

Result: Dialed digits are sent across the PSTN then sent through the host PBX to host station 3.

Call scenario 2: host-controlled—external corporate call

The following diagram shows how a call is routed when making a host-controlled call to a party outside the organization.



G101393

The network used to route the call is transparent to the user, and the dialing requirement is the same for both. Calls work the same way in reverse, through the host PBX site to the Remote Gateway 9150 site.

Voice over IP network call

- 1 User 1 presses the host call appearance key.

Result: User 1 hears a dial tone. This indicates that the connection to the RLC over the IP network was successful.

- 2 User 1 dials the external telephone number.

Result: The dialed digits are sent by the Remote Gateway 9150 unit as packets across the Ethernet network. The RLC converts the packets to the format required by the PBX. The PBX then converts the data to voice and routes the call through the PSTN to the called party.

PSTN call

- 1 User 3 presses the host call appearance key.

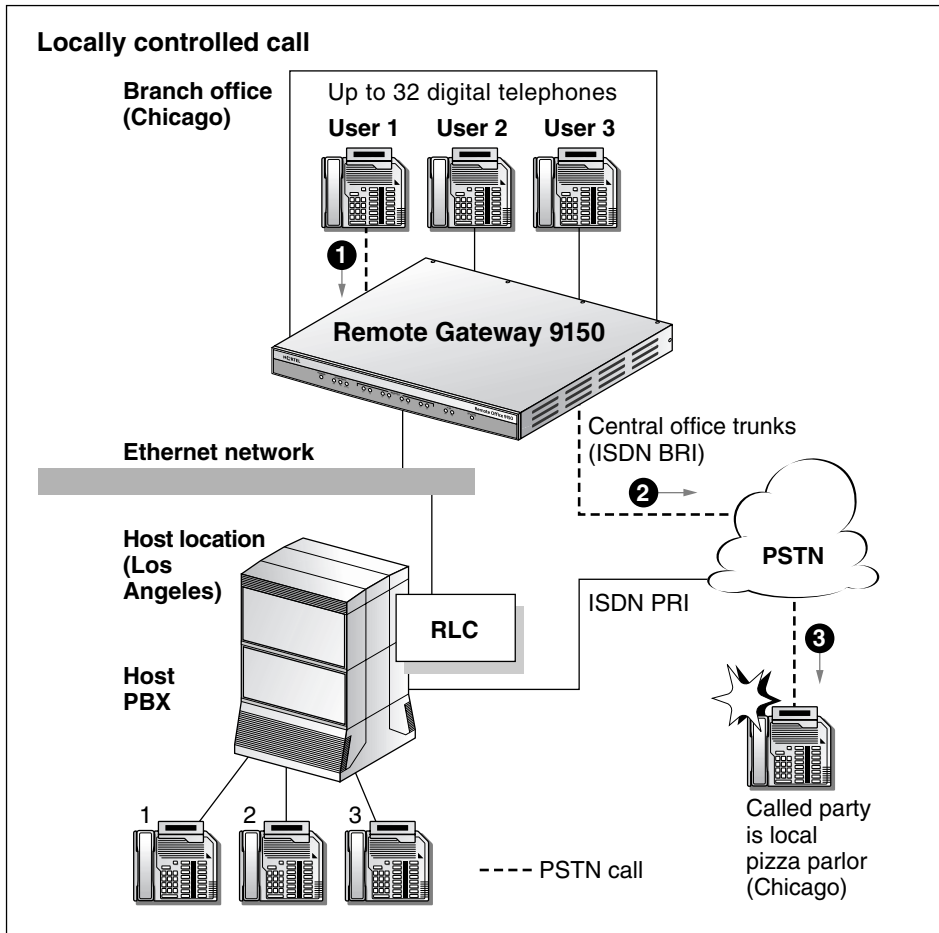
Result: User 3 hears a dial tone. This indicates that the connection to the RLC over the PSTN was successful.

- 2 User 3 dials the external telephone number.

Result: Dialed digits are sent across ISDN BRI through the PSTN, through the host PBX to the called party.

Call scenario 3: locally controlled mode—local call

The following diagram shows how a call is routed when making a call within your local area.



G101394

Local call

- 1** User 1 presses the local call appearance key and hears a dial tone from the Remote Gateway 9150 unit.
- 2** User 1 then dials a trunk access code (such as #61) and hears a dial tone from the Central Office (PSTN).

Note: If all trunks are busy and unavailable, then User 1 hears a fast busy signal.

- 3** User 1 dials the telephone number (the pizza parlor in this example). The dialed digits are sent across the ISDN BRI connection through the PSTN to the called party.

Telephones

This section lists the telephones, modules, and related applications supported by the Remote Gateway 9150 unit. This section also describes some of the basic characteristics of these elements of a Remote Gateway 9100 Series system.

Supported digital telephone sets

The Remote Gateway 9150 unit supports following Meridian digital telephone sets:

- | | | |
|------------|---------|---------|
| ■ M2008D | ■ M3110 | ■ M3902 |
| ■ M2008HFD | ■ M3310 | ■ M3903 |
| ■ M2216D | ■ M3820 | ■ M3904 |
| ■ M2616D | ■ M3901 | ■ M3905 |

Notes:

1. Because it is a discontinued model, the M2616CT cordless digital telephone set is no longer supported.
2. When you update the message on the host PBX that displays when the digital telephone set is idle, you must unplug the digital telephone set and plug it back in for the change to take effect.

Notes for M2xxx series digital telephone sets:

1. The M2006 digital telephone set is also supported, but can be used only for locally controlled calls.
2. Auto Answer Back (AAB) activation on M26xx series digital telephone sets on Remote Gateway 9100 Series units connected to CS 2100 PBXs does not produce a dial tone. The digital telephone sets operate properly, but no dial tone is present. To produce dial tone in this situation, configure the port on the RLC as a TAPI port.

Notes for M39xx series digital telephone sets:

1. If you want to use an M3901 digital telephone set for remote (host-controlled) calls, you must configure the digital telephone set as an M3901 at the remote unit and as an M3902 at the host PBX. For local calls, you must configure the M3901 digital telephone set as an M3901 at both the remote unit and the host PBX.
2. To label the Local Keys on M3902 digital telephone sets, use the options key on the digital telephone set itself.
3. The M3904 digital telephone set Key Map fails using Virtual Office on Remote Gateway 9100 Series. Upgrade the digital telephone set's firmware to version 7.9 to resolve this problem.
4. Uploading and downloading M3904 and M3905 firmware requires the most recent digital telephone set hardware. To resolve problems following firmware uploads and downloads, including missing functionality, refer to the User Guide and Release Notes for your particular digital telephone set.
5. When logging on to an ACD queue using an M3905 digital telephone set connected to a Remote Gateway 9150 unit, the logon process takes longer than expected if a headset is not plugged into the digital telephone set. Initialization of the digital telephone set under these conditions can take up to one minute.
6. Phase I M3905 digital telephone sets receive false messages during a reboot of the Remote Gateway 9150 unit and can lock up. Unplug and re-plug the telephone cord at the wall jack or perform a system shutdown and re-power up the Remote Gateway 9150 unit to recover. This is not a problem with Phase III M3905 digital telephone sets.
7. When you answer an incoming local call on an M39xx digital telephone set, the call log records the calling DN. However, you cannot dial directly from the Call Log, as the trunk access code and country code do not always appear. To resolve this, navigate through the call log to the number that you want to dial. Press the **Edit** key and the digit(s) of the missing code(s). Press the **Done** key. To dial the revised number, press the **Dial** key.

For example, the call log for an ISDN number displays the digits 4445551212. The missing trunk access code (9) and country code (0) are required to dial the number. Use the Edit key to enter the missing digits, 9 followed by 0. The number now appears in the M39xx's LCD display as 904445551212. The end-user can now press the Dial key to place the call from the call log.

8. If you downgrade the host PBX to a release prior to X11 release 25.40, you must also downgrade any new or upgraded M39xx digital telephone sets so that the Meridian 1 PBX can support them. This applies to digital telephone sets attached to Remote Gateway 9100 Series units and Extended Digital Line Cards.
9. Flash upgrade download times to remote M39xx digital telephone sets over an IP network with low delay and packet loss are comparable to PBX wired downloads. Using PSTN bandwidth on a Remote Gateway 9150 unit or a Remote Gateway 911x series unit, download times increase.

M2000 series (M3310, and M3820 European models) and M39xx series digital telephone set model and accessory compatibility

Digital Telephone Set Models ⁱ	Compatibility with Remote Gateway 9150 units
M2006	✓
M2008D, M2008HFD	✓
M2616D	✓
M2216D-ACD	✓
M2616CT Cordless	Discontinued
M3310, M3820 (Europe only)	✓
M3901 ⁱⁱ	✓
M3902, M3903	✓
M3904	✓
M3905 (ACD)	✓
M2000 series (M3310 & M3820 European models) Add-on Modules	
Headsets	✓
External alert	✓
Key-based expansion module	✓
ATA (Analog Terminal Adapter) ⁱⁱⁱ	✓
MCA (Meridian Communications Adapter)	✓

i. The host PBX must be running software capable of supporting each digital telephone set model used.

ii. Refer to the Meridian digital telephone hardware compatibility section of the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for required configuration details.

iii. ATA modules support analog telephone sets and facsimile (FAX) machines. ATA modules do not support modems.

M39xx series digital telephone set accessory compatibility

The following table shows Remote Gateway 9150 unit compatibility with M39xx series digital telephone set accessories.

M39xx series Digital Telephone Set Accessories and Add-on Modules	Compatibility with Remote Gateway 9150 units
Headsets	✓
External alert & recording interface	✓
Key-based expansion module (22-button, up to two per 3904/05)	✓
Display-based expansion module	✓
ATA (Analog Terminal Adapter) ⁱ	(Refer to Note i)
Personal Directory PC utility	✓
Full-duplex Speakerphone	✓
CTI (Computer Telephony Integration) Adapter	✓

i. The Remote Gateway 9150 unit supports ATA modules. These modules support analog telephone sets and facsimile (FAX) machines. They do not support modems.

Supported telephone modules

The following telephone modules are supported:

- add-on modules (to add more keys)
- application modules that provide more functionality
- Meridian Communication Adapters (MCA)
- Analog Telephone Adapters (ATA)

Notes:

1. You cannot dial host PBX calls from the Call Log of M39xx series digital telephone sets because the Trunk Access code and country code can be not displayed. You cannot dial local calls from the Call Log of the M39xx series digital telephone sets because the information contained in the Call Log does not contain trunk group information.
2. After re-boot of a Remote Gateway 9150 unit, re-boot each ATA as well.

Computer telephony integration (CTI) applications

There are two types of CTI applications:

- first-party CTI applications that use the Symposium Desktop TAPI Service Provider
- third-party CTI applications that use Symposium TAPI Service Provider for the Meridian 1 PBX

Both types can be used with the Remote Gateway 9150 unit.

TAPI Type	Supported CTI Application
Symposium Desktop TAPI Service Provider 1.6	<ul style="list-style-type: none">■ Symposium FastView 1.6■ Symposium FastCall 1.6■ Symposium Call Manager 5.0■ other TAPI-compliant applications
Symposium TAPI Server Provider for Meridian 1 PBX release 2.1	<ul style="list-style-type: none">■ Symposium Agent 1.1■ Symposium Call Manager 5.0■ other Symposium Partner products

You can use first-party CTI applications with the Remote Gateway 9150 unit if

- your PC is equipped with a Symposium Communicator card version 1.2 with software version 2.0
- your digital telephone is equipped with a Meridian Communications Adaptor (MCA)

Note: The Symposium Communicator card is not available in all countries. Check with your Nortel distributor for availability.

Automatic Call Distribution (ACD) applications

The Remote Gateway 9150 unit supports all Nortel ACD applications.

If an ACD agent loses communication to the Remote Gateway 9150 unit, or the unit goes offline, the agent is placed in Make Set Busy (MSB) mode. This mode logs the agent out of the ACD queue so that calls can be routed to other ACD agents. Once you re-establish communication between the agent and the Remote Gateway 9150 unit, the digital telephone set display shows “Set Busy Activated”.

In addition, when an ACD agent is on a call using a Local Calling key, the Remote Gateway 9150 unit sends a transparent Not Ready key press to the host PBX and places the ACD agent’s digital telephone set in Not Ready mode. This feature prevents the ACD agent from receiving ACD calls when active on a local call. The Remote Gateway 9150 unit removes the digital telephone set from the Not Ready mode when the agent terminates the local call.

If you are having trouble with ACD agents being logged off unexpectedly or calls that terminate prematurely, try the following:

- Set the User On Demand Idle Timer to 90 seconds and the User On Demand Minimum Call Timer to 1 second.

Note: You can configure these settings on the RLC’s Remote Connection Configuration property sheet in Configuration Manager.

- Allocate a permanent connection for the ACD agents.
 - On the RLC Port Configuration property sheet, click on the **Configure** button for the Network Port in question.
 - In the Network Port Configuration dialog box, select Permanent Allocation.

Voice over IP features

You can configure the Remote Gateway 9150 unit to use the following Voice over IP (VoIP) features:

- Convert analog voice into digital data for transmission as voice packets over the network for calls to or from the fax machine or other analog device that is connected to the analog port on Telco 1.

- Automatically switch from the IP network to the PSTN when the voice QoS on the IP network falls below a predetermined threshold, and back to the IP network when the QoS returns to normal.

Packetized voice

DSPs located in the Remote Gateway 9150 unit convert voice into digital data packets and, if compression is used, compresses them. The data is constructed as UDP/IP voice packets for transmission over the IP network.

When voice packets are compressed, they consume less bandwidth, leaving more bandwidth for data or other voice or fax communications. The following algorithms are supported:

- G.711: Packets are transmitted at 64 Kbps (that is, they are not compressed).
- G.726: Packets are compressed and transmitted at 32 Kbps.
- G.729A: Packets are compressed and transmitted at 8 Kbps.

G.729A is the default algorithm on both the RLC and the Remote Gateway 9150 unit.

In addition to voice compression, the Remote Gateway 9150 unit supports the following additional packetized voice features:

- A voice jitter attenuation buffer removes the variable delays from the voice packets sent across the IP network, thus avoiding awkward-sounding speech.
- Packet loss handling techniques accommodate missing packets or packets received too late to be processed.
- Silence suppression prevents packet transmission during periods when there is no voice data present. Comfort noise is inserted to assure the user that the line is still active.

Silence is determined when the difference between the adaptable noise floor and the detected signal is less than 9 dB. To prevent clipping, silence must be present for a minimum of 250 milliseconds.

QoS Transitioning Technology

Communications between the Remote Gateway 9150 unit in your office and the host PBX take place across the IP network using a 10BaseT Ethernet interface. You can configure the Remote Gateway 9150 unit to switch automatically from the IP network to the PSTN when the voice QoS falls below a predetermined threshold. Within the QoS settings, you can also enable Differentiated Services (DiffServ) and 802.1Q Mapping to give priority to voice over IP traffic on your network.

Both the RLC and the Remote Gateway 9150 unit monitor the IP network's QoS constantly. If the IP network QoS degrades, causing poor voice quality, the Remote Gateway 9150 unit moves, or transitions, the call to the PSTN. When the QoS returns to normal, the Remote Gateway 9150 unit transitions the call back to the IP network.

QoS transition recovery

Due to the requirement for on-demand router support, the IP network is not continually tested during QoS transition situations. It is tested only when there are active voice calls over the PSTN. As a result, to switch back to the IP network, QoS Transitioning Technology needs active calls for the user-configured recovery period.

If you test QoS transition by disconnecting the Ethernet cable from the Remote Gateway 9100 Series unit, or RLC, expect up to a 20-second delay before the Remote Gateway 9100 Series unit can place or receive a call. You do not encounter this delay when the network degrades and calls switch to BRI as designed.

For detailed instructions on configuring the thresholds, refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210). For guidelines on evaluating and adjusting the QoS on your IP network, refer to the *Remote Gateway 9100 Series Network Engineering Guidelines* (NTP 555-8421-103).

Voicemail messages and Quality of Service transitions

It can take several seconds of sustained errors to cause a Quality of Service (QoS) transition to the PSTN. During this time, voice quality may suffer due to errors. If a message to a voice mailbox is being recorded during these errors, portions of the message can be unintelligible.

Log reports and statistics

Configuration Manager provides a statistics log that identifies the number of QoS transitions (refer to “Caller Info Statistics” on page 300).

Refer to *Chapter 7, “Administration”* for a detailed description of log and statistic reports.

Port management

You can assign Remote Gateway 9150 stations to one of the following types of RLC ports:

- single-user ports
- multi-user voice ports
- dynamic port pool

Port types are assigned on the RLC. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for detailed instructions.

Single-user ports

Each port that is defined as a single-user (dedicated) port on the RLC supports one Remote Gateway 9150 station.

Multi-user ports

Ports that are defined on the RLC as multi-user ports allow multiple stations on different Remote Gateway 9150 units to time-share a single port on the host PBX.

Up to eight persons can share the same RLC port, but not at the same time. All stations that use this type of port must respond to the same DN and have identical telephone set configurations. This port type is especially useful for employees who work mutually exclusive shifts.

Dynamic port pool

Dynamic port pooling is similar to a multi-user port except that the persons who share ports in a dynamic pool are assigned to the next available port in the RLC port pool. There is no correlation between the station and the port on the RLC.

This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

Station priority

You can define the priority of a station's assigned RLC port as normal, high, IP only, or circuit only.

Normal priority

When both the IP and PSTN networks are used to route calls, calls to and from the station are routed primarily over the IP network. Calls transition between the IP and PSTN networks whenever voice QoS levels change. (The voice QoS levels are defined on the Quality of Service screen on the RLC for your Remote Gateway 9150 unit.)

High priority

When you define an RLC port as high priority, the associated station has the following benefits:

- If allowed to use the IP network to process calls (this is transparent to the user), an active call on that station is always one of the first to transition to PSTN trunks when Voice over IP QoS degrades. (This transition is accomplished using the QoS Transitioning Technology.)
- Call blocking is reduced because bandwidth is always available to these stations.

Note: If the reserved bandwidth is being used by other high priority stations, then new calls are processed using unreserved bandwidth.

The number of stations that you can configure as high priority depends on the amount of available bandwidth. Ensure that enough bandwidth is available to process calls on normal priority stations.

IP only

Calls to and from the station are routed over the IP network only. QoS transitioning is not available for stations that are defined as IP only.

Circuit only

Calls to and from the station are routed over the PSTN network only. Circuit only stations never experience voice QoS degradation.

Connection bandwidth

On the connection between the RLC and the Remote Gateway 9150 unit, you can configure the following:

- when to open additional B-channels (referred to as *extra bandwidth*)
- how much bandwidth to reserve for high priority stations (referred to as *priority reserved bandwidth*)

For instructions, refer to “Configuring ports” in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Extra bandwidth

When available bandwidth is no longer sufficient to process active calls, additional B-channels are opened according to the extra bandwidth setting. For example, if you configure the extra bandwidth setting as 16 Kbps, another B-channel opens when existing bandwidth is reduced to 16 Kbps or less.

Priority reserved bandwidth

The priority reserved bandwidth setting defines how much bandwidth to reserve for high priority stations. The reserved bandwidth cannot be used by stations configured as normal, IP only, or circuit-only priority. High priority stations consume priority reserved bandwidth before consuming unreserved bandwidth.

For example, if you configure the priority reserved setting as 16 Kbps, then only high priority stations can use this reserved bandwidth. When the reserved bandwidth is being used for active high priority calls, additional calls from high priority stations are processed using unreserved bandwidth. If no bandwidth is available, calls to or from high priority stations are blocked until bandwidth becomes available.

Local calling

The Remote Gateway 9150 unit allows you to place calls to other extensions within your office or to telephones in your local community. This is accomplished through the use of up to two local call appearance keys. Refer to Chapter 6, “Using Remote Gateway 9150 stations,” for a detailed description of the local call appearance keys.

The Remote Gateway 9150 unit discovers the DN numbers of the local digital telephones either through DN Discovery or configuration. The Bridge Ports, Local Calling, and Local SwitchOver features depend on this knowledge as follows:

- If a call has an appearance on a Local Calling key, the Remote Gateway 9150 unit first attempts to complete the operation (for example, call, transfer, forward) using the local dialing plan.
- If a call is placed from a Local Calling key to a number not found in the Remote Gateway 9150 unit's local list, then a Bridge Port is used to place the intended call to the host PBX.

Local extension calling

When you place a call to another telephone in your office using the local call appearance key, it is handled by the Remote Gateway 9150 unit, not the host PBX.

Note: If the call is initiated from the host call appearance key, then the station-to-station call requires transmission of signaling data through the host PBX.

Local SwitchOver

Local SwitchOver is a mechanism that the Remote Gateway 9150 unit uses to determine if a PBX-controlled call that originated on the Remote Gateway 9150 unit is destined for a DN on the same Remote Gateway 9100 Series unit.

Note: The DN Discovery feature is necessary for the Local SwitchOver feature to work properly. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for more information.

In this situation, the Remote Gateway 9150 unit switches to a local 64K channel and cross-connect the voice-paths of the phone without using wide area bandwidth.

There are times, however, when the Remote Gateway 9150 unit does not know that an incoming and outgoing call are part of the same call (for example, you transfer/forward a call within the same PBX, or re-dial the last number). Although the call still functions, it consumes Wide Area bandwidth.

Local SwitchOver is not available if the call is answered with the Handsfree button on M39xx telephones.

Local calls through PSTN

The Remote Gateway 9150 unit allows you to place outgoing and answer incoming PSTN calls over the ISDN BRI connection.

Refer to Chapter 6, “Using Remote Gateway 9150 stations,” for a more detailed description of local calling.

Bridge Port

Bridge Ports are proxy ports that represent local calls or inbound PSTN calls to the PBX. When a local call on a Remote Gateway 9150 unit needs PBX services, the Bridge Port obtains a PBX presence on behalf of the local call.

Call restrictions

To prevent outgoing calls to certain types of numbers (for example, 1-976), you can disable outgoing calls to specific digit sequences.

Supported digital telephone features

Remote Gateway 9100 Series supports the following Meridian digital telephone features for locally controlled calls:

- Paging
- Call Waiting
- Hold for calls that appear on local call appearance keys
- Call Transfer (blind and announced) for station-to-station calls only
- Release
- Handsfree
- calling line identification (CLID) and calling party name display (CPND)

Unsupported telephone features

Remote Gateway 9100 Series does not support Distinctive ring functionality of any kind.

Digital telephone features requiring Bridge Ports

You must configure Bridge Ports for Remote Gateway 9100 Series to support the following Meridian digital telephone features for locally controlled calls:

- Conference
- Call Forward

Online/offline table

The online/offline table is configured on the RLC and allows you to schedule times

- when the ISDN BRI connection to the host PBX is made available to the Remote Gateway 9150 site

Note: When the Remote Gateway 9150 unit is in offline mode, users cannot place or receive calls through the host PBX over the IP or PSTN.

- when all telephones at the Remote Gateway 9150 site revert to normal telephone service

This allows you to ensure that unwanted ISDN BRI telephone calls through the host PBX are disabled after business hours.

How the table works

You can define up to eight entries per day, every day of the week, for each remote site. You can define each entry as online, offline, or undefined for each time period entered.

Users at the Remote Gateway 9150 site can override the settings of the online/offline table, if the table attempts to suspend access to the host PBX in the middle of a business call. Each user station at the remote site is alerted by a buzz and a display message at 30, 20, and 10 seconds before the connection is terminated. To override connection termination, the user must enter the online SPRE (Special Prefix) code on the telephone.

Configuration

The online/offline table is configured for each remote site on the RLC. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for configuration information.

For a description of how to go online or offline at the Remote Gateway 9150 site, refer to Chapter 6, “Using Remote Gateway 9150 stations.”

Other supported features

In addition to the features described in the previous sections, the Remote Gateway 9150 unit also supports the following features:

Fax support

The Remote Gateway 9150 unit contains one analog port that can be used to send and receive faxes. You can send and receive faxes in both host- and locally controlled call modes over the IP or PSTN.

To support faxing through the host PBX, the fax port on the Remote Gateway 9150 unit must be associated with a port on the RLC that is configured on the host PBX with voice capability.

Emergency activation code

If your community has implemented an emergency service number (such as 911) to call the police, fire department, or ambulance, you can configure that number on the Remote Gateway 9150 unit. This allows users in your office to dial the emergency number and be connected directly to the local emergency dispatch center through the PSTN. The call is automatically routed through the local PSTN without having to dial a local trunk access code.

When you configure an emergency activation code on the Remote Gateway 9150 unit, you also prevent the call from being automatically routed through the host PBX. This is because the PBX can be in a different city. An emergency call that is routed through the host PBX can result in emergency support being dispatched to the wrong location.

ATTENTION!

If you are using only the IP network to route calls, place emergency service calls on a telephone that is directly connected to a PSTN line. If you place an emergency service call from a station that is connected to the Remote Gateway 9150 unit, the call is routed through the host PBX. If the PBX is in a different city, the call contacts the wrong emergency services.

Communications system and software requirements

The following table shows the software versions necessary to run Remote Gateway 9150 units on compatible Nortel's communications systems.

Remote Gateway 9150, Remote Gateway 911x series, and Digital Telephone IP Adapter units

Communications system ⁱ	System software version
Meridian 1 PBX	X11 release 23 or higher
CS 1000	Release 2 or higher
CS 2100	Release MSL12 or higher
1. Requires Remote Gateway 9100 Series software version 1.5 or higher.	

Supported Codecs

The following tables show the Codecs supported by the Remote Gateway 9100 Series and Digital Telephone IP Adapter units, as well as the data stream, and approximate peak bandwidth required by each.

Remote Gateway 9150 units

CODEC	Data stream only	Approximate total bandwidth, including IP overhead (30 ms voice packets)
G.711	64 Kbps	78 Kbps
G.726	32 Kbps	44 Kbps
G.729A	8 Kbps	22 Kbps

Administration software

Configuration and administration of the Remote Gateway 9150 unit is performed with Configuration Manager software, a Windows-based application that is installed on your PC.

The software is provided on the Remote Gateway 9100 Series Product CD-ROM. You can obtain the CD from your Nortel distributor or click on the Support link at the following website:

www.nortel.com

Administration PC connection options

You can connect the administration PC to the Remote Gateway 9150 unit through the following:

- an RS-232 connection to the administration PC's serial port
- a 10BaseT Ethernet interface connection

Remote Gateway 9100 Series Configuration Manager

Remote Gateway 9100 Series Configuration Manager allows you to configure the Remote Gateway 9150 unit. It also provides the Configuration Wizard for first-time configuration. The Configuration Wizard prompts you for the minimum information that is needed to get the Remote Gateway 9150 unit communicating with the RLC on the host PBX. After the initial configuration is completed, use Configuration Manager to administer the Remote Gateway 9150 unit. Administration tasks include the following:

- viewing the system status
- performing upgrades, backups, or restores
- making configuration changes
- changing the administration password

Note: Configuration Manager alerts you when you must restart after you have made a configuration change.

Command line interface

When the administration PC is connected to the Remote Gateway 9150 unit through the serial port, you can view the command line interface using an application such as Telnet or HyperTerminal. However, the command line interface is not documented in this guide. Configuration Manager is the supported tool for administering the Remote Gateway 9150 unit over both the serial port and Ethernet connections.

Chapter 2

Planning for Remote Gateway 9150 unit installation

In this chapter

Remote Gateway 9150 Installation Checklist	46
Physical environment	50
Network considerations	55
Administration PC	59
Trunk connection management	64
Station configuration	66
Security	70
Planning for future growth	72
Deployment options	75
Planning the configuration	81

Installation checklist

When you are preparing to install your Remote Gateway 9150 unit, use the following checklist to ensure that you complete all the required processes properly.

Remote Gateway 9150 Installation Checklist

Page 1 of 4

✓	Task	For details, refer to
<input type="checkbox"/>	Review the <i>Release Notes</i> for last-minute product updates.	<i>Remote Gateway 9100 Series and RLC Release Notes</i> (NTP 555-8421-102).
<input type="checkbox"/>	Ensure you have the latest firmware and software.	<i>Remote Gateway 9100 Series and RLC Release Notes</i> (NTP 555-8421-102)
<input type="checkbox"/>	You can route calls over the IP network, the PSTN, or both. Determine, at a high level, what you must do to implement these call routing methods.	“Deployment options” on page 75.
<input type="checkbox"/>	If you want to use the IP network to route calls, evaluate the IP network to determine if the network infrastructure can support voice traffic.	<ul style="list-style-type: none"> ■ your data network administrator ■ <i>Remote Gateway 9100 Series Network Engineering Guidelines</i> (555-8421-103)
<input type="checkbox"/>	If you want to use the PSTN to route calls, order trunks from the central office to the Remote Gateway 9150 unit site.	“ISDN BRI information” on page 82.
	Note: The Remote Gateway 9150 unit supports ISDN BRI trunks (S/T or U interface).	

Remote Gateway 9150 Installation Checklist

Page 2 of 4

✓	Task	For details, refer to
<input type="checkbox"/>	Obtain the cables that you need to establish the network connections.	“Cables you must supply yourself” on page 53.
<input type="checkbox"/>	Decide on the administration PC setup.	“Administration PC” on page 59.
<input type="checkbox"/>	Gather the configuration information (network addresses, connection numbers, online/offline schedule, QoS thresholds, and so on).	<ul style="list-style-type: none"> ■ “Deployment options” on page 75 ■ Appendix A, “Planning forms”
<input type="checkbox"/>	Install DSP application and trunk interface modules into the Remote Gateway 9150 unit.	“Installing trunk interface or DSP application modules” on page 93.
<input type="checkbox"/>	Choose a suitable location for the Remote Gateway 9150 unit.	“Choosing a suitable location” on page 98.
<input type="checkbox"/>	Install the Remote Gateway 9150 unit in the chosen location.	“Installing the Remote Gateway 9150 unit” on page 98.
<input type="checkbox"/>	Connect the Remote Gateway 9150 unit to the power source, administration PC, and network.	“Connecting the Remote Gateway 9150 unit” on page 105.
<input type="checkbox"/>	Power up the Remote Gateway 9150 unit and observe LED indicator behavior. The Status LED indicator remains lit when the power-up cycle completes successfully.	“Powering up the Remote Gateway 9150 unit” on page 111.

Remote Gateway 9150 Installation Checklist

Page 3 of 4

✓	Task	For details, refer to
<input type="checkbox"/>	Install the software from the product CD-ROM or the Nortel web site.	“Installing the Configuration Manager software” on page 113.
<input type="checkbox"/>	Configure the IP address, subnet mask, and default gateway on the Remote Gateway 9150 unit.	“Using the Configuration Wizard to perform initial configuration” on page 115.
<input type="checkbox"/>	Configure the following items, as required, to create the communication paths between the Remote Gateway 9150 unit and the RLC: <ul style="list-style-type: none"> ■ IP network: RLC’s IP address ■ PSTN: <ul style="list-style-type: none"> — RLC’s telephone number — primary trunk ■ security level and, if required, security identifier 	<ul style="list-style-type: none"> ■ “Using the Configuration Wizard to perform initial configuration” on page 115 ■ “Security level configuration” on page 200
<input type="checkbox"/>	PING the Remote Gateway 9150 unit and ensure that it is recognized as a device on the network.	“Testing the network connections” on page 129.
<input type="checkbox"/>	Ensure that the Remote Gateway 9150 unit’s connection information is completed on the RLC.	the <i>Reach Line Card Installation and Administration Guide</i> (NTP 555-8421-210).
<input type="checkbox"/>	Configure user stations with appropriate calling permissions and features.	“9150 port configuration” on page 207.

Remote Gateway 9150 Installation Checklist

Page 4 of 4

✓	Task	For details, refer to
<input type="checkbox"/>	Configure ports on the RLC.	the <i>Reach Line Card Installation and Administration Guide</i> (NTP 555-8421-210).
<input type="checkbox"/>	Configure network devices <ul style="list-style-type: none"> ■ so that voice traffic is not constrained or congested ■ to maximize network efficiency for Voice over IP service 	<ul style="list-style-type: none"> ■ your data network administrator. ■ <i>Remote Gateway 9100 Series Network Engineering Guidelines</i> (555-8421-103)
	Ensure that voice calls can be sent or received over the following:	your data network administrator.
<input type="checkbox"/>	<ul style="list-style-type: none"> ■ IP network 	
<input type="checkbox"/>	<ul style="list-style-type: none"> ■ PSTN 	
<input type="checkbox"/>	Ensure that processing of voice and data traffic over the IP network performs as expected.	<ul style="list-style-type: none"> ■ your data network administrator ■ your telecom network administrator
<input type="checkbox"/>	Adjust QoS Transitioning Technology settings, if required.	<ul style="list-style-type: none"> ■ <i>Remote Gateway 9100 Series Network Engineering Guidelines</i> (555-8421-103)
<input type="checkbox"/>	Ensure that calls can be made and received on each station.	“Testing the network connections” on page 129.
<input type="checkbox"/>	Plan for administration training and technical support.	<ul style="list-style-type: none"> ■ Chapter 7, “Administration” ■ Chapter 8, “Troubleshooting”

Physical environment

This section provides the space, temperature, cabling, and mounting information you need to know before you install the Remote Gateway 9150 unit.

Space

Ensure that the Remote Gateway 9150 unit is installed in a location that is dry and provides plenty of air circulation.

The chosen location must be no more than cable-length distance from the following:

- the administration PC (if the serial connection is used)
- the Ethernet hub
- trunk and telephone connection interfaces

The Remote Gateway 9150 unit can be installed up to

- 1230.7 meters (4000 feet) from the digital telephones
- 307.7 meters (1000 feet) from the analog device

It is recommended that you install the Remote Gateway 9150 unit in the same room where your communications equipment is installed.

Temperature and humidity

The following table describes the temperature and humidity conditions that the Remote Gateway 9150 unit can withstand without any performance degradation or damage.

Specification	Minimum	Maximum
Normal operation		
Recommended:		
■ Temperature (Ambient)	■ 0°C (32°F)	■ 40°C (104°F)
■ Relative humidity	■ 5%	■ 95% (non-condensing)
Storage		
Recommended temperature	-40°C (-40°F)	70°C (158°F)
Relative humidity	5%	95% (non-condensing)

Mounting options

You can place the Remote Gateway 9150 unit on a desk or in a rack, or you can mount it on the wall.

The Remote Gateway 9150 unit dimensions are

- 42.5 cm (17 in.) wide (without rack-mounting brackets)
- 29.4 cm (11.75 in.) deep
- 4.4 cm (1.75 in.) high

Mounting the Remote Gateway 9150 unit in a rack

If you want to install the Remote Gateway 9150 unit in a rack, the rack slot must

- be large enough to provide air circulation to keep the Remote Gateway 9150 unit cool
- allow you to securely fasten the Remote Gateway 9150 unit to the rack using the rack-mount brackets

Mounting the Remote Gateway 9150 unit on the wall

If you want to install the Remote Gateway 9150 unit on the wall, you can mount it so the cables from the rear panel are directed either right or left. Ensure that the chosen location allows you to easily view the LED indicators on the front panel.

ATTENTION!

You must complete wall installation using standard telephony installation practices.

Connections

The following connections are made from the rear panel of the Remote Gateway 9150 unit to the telephone and data networks:

- Two 25-pair connectors (labeled TELCO 1 and TELCO 2) provide tip and ring connections to stations (telephones) and central office trunks (ISDN BRI). These connections provide the interface to the telephone network and the PSTN.

- An RJ-45 connector (labeled ETHERNET) provides a 10BaseT Ethernet connection. This connection provides the ability to pass both voice and data administration traffic over the existing Ethernet network.
- A DB-9 connector (labeled ADMIN) provides an RS-232 serial port connection. You can use this serial port connection to configure a Remote Gateway 9150 unit that is directly connected to a PC.

Cables included with the Remote Gateway 9150 unit

The Remote Gateway 9150 unit package includes the following cables:

- power cord and power supply

Notes:

- In North America, the power cord and power supply are included inside the Remote Gateway 9150 box. In all other regions, the power supply is provided inside the box. However, the power cord for your region is provided outside the box.
- When the North American power cord and power supply are connected together, they are 3.2 meters (10.4 feet) in length.
- If you connect the Remote Gateway 9150 unit to an uninterruptible power supply then the UPS must have a minimum of 100 Watts available.

- RS-232 serial cable

If the RS-232 cable is not long enough, you can supply your own cable, up to 15.38 meters (50 feet) in length.

Cables you must supply yourself

The cables used to establish the telephone and Ethernet network connections are industry-standard cables. They are not provided in the Remote Gateway 9150 package. You must obtain them from your local cable supplier.

Telephone network cables

The telephone network cables establish the telephone and trunk connections.

One end of the cable must provide a male 50-pin connector. (This end connects to the Remote Gateway 9150 unit.)

Ensure that the other end of the cable matches the connectors needed to connect to the telephones or trunks. (For example, if you are using a BIX block to establish the telephone connections, you might need to cut off the connector to expose the wires inside.)

Notes:

- Two telephone cables may be required, based on how many telephones and ISDN BRI lines you plan to connect. (Each telephone cable provides support for up to 16 digital telephones, and two ISDN BRI lines providing two B-channels each. The Telco 1 cable also provides support for one analog station such as a fax machine.)
- The Telco 1 and 2 connections are the opposite gender of the connections for a Meridian 1 PBX IPE or Meridian 1 PBX 11 cabinet line card slot. Therefore, you must use different cables when connecting to the Remote Gateway 9150 unit than those used to connect to Meridian 1 PBX line cards.
- Digital telephones must be located no farther than 1230.7 meters (4000 feet) from the Remote Gateway 9150 unit.
- The analog device must be located no farther than 307.7 meters (1000 feet) from the Remote Gateway 9150 unit.

Ethernet cable

If you are connecting the Remote Gateway 9150 unit to a hub, you need a standard CAT5 un-shielded twisted-pair (UTP) straight-through Ethernet cable. The cable must be no longer than 100 meters (325 feet) in length.

Network considerations

The Remote Gateway 9150 unit communicates through both the IP and telecommunications network using a host PBX.

To use the Remote Gateway 9150 unit in these networks, you must consider the issues described in this section.

IP addressing and routing

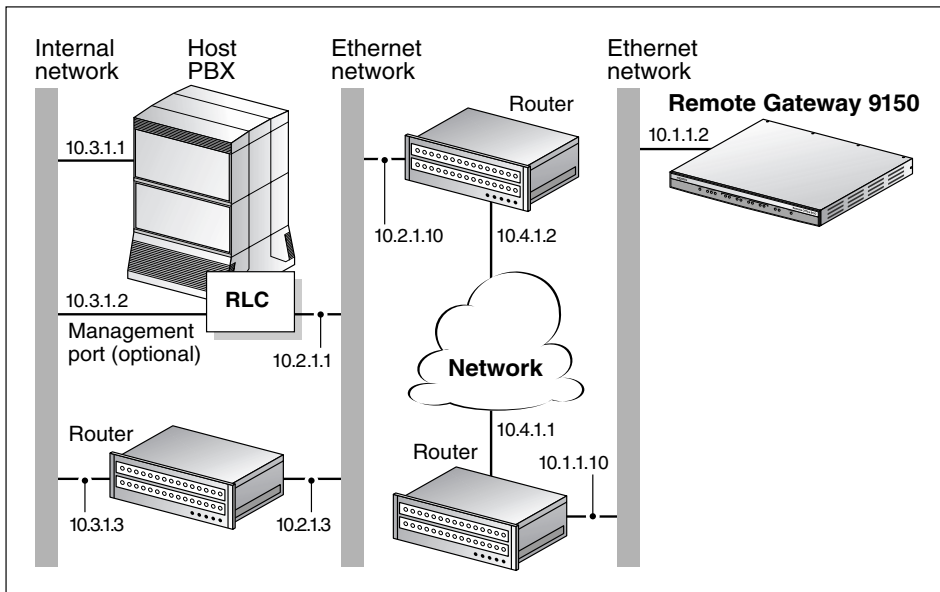
To place and receive calls over the IP network, the Remote Gateway 9150 unit must have:

- a physical connection to the IP network
 - a unique IP address, default gateway, and subnet mask
- Note:** Similarly, you must assign a unique IP address, default gateway, and subnet mask to the RLC on the host PBX.

In addition, the Remote Gateway 9150 unit must be able to send and receive traffic to and from the RLC on the host PBX.

Network diagram

The following diagram shows the Remote Gateway 9150 unit's position in an IP network.



G101418

Note: For placement of one or more administration PCs, refer to “Administration PC” on page 59.

QoS

The routers used on your IP network must be capable of handling voice traffic, with little or no congestion and few delays. If the network is congested or subjected to many delays, voice quality is affected.

For more information, refer to the *Remote Gateway 9100 Series Network Engineering Guidelines* (555-8421-103).

Numbering plans

Each trunk group at the Remote Gateway 9150 unit site must be assigned a trunk access code (that is, the number dialed to obtain an outgoing trunk). In addition, special prefix (SPRE) codes must be defined for the following features if you want to use them:

- paging
- local calling on ATA-equipped analog devices
- to go online or offline (for more details, refer to “Online/offline table” on page 40)
- registration and deregistration for multi-user or dynamic ports

All trunk access and SPRE codes are automatically defined in Configuration Manager with a pound prefix (# in North America) so that there are no conflicts with host PBX dialing plans. For a list of the default trunk access and SPRE codes, refer to the “Remote Gateway 9150 Configuration Information—Dialing Plans” form on page 384.

Numbering plan for local stations

Consider the numbering plan on the host PBX when setting up the numbering plan for local stations at the Remote Gateway 9150 unit site. This ensures that station-to-station calls through the host PBX complete correctly.

Call blocking

Call blocking can occur when there are more users installed and more calls being processed than can be supported by the Remote Gateway 9150 unit’s DSP application and trunk interface modules.

The voice processing capacity of the remote system depends on the number of DSP application and trunk interface modules installed in the Remote Gateway 9150 unit and the amount of bandwidth available to process calls. If bandwidth is not available, additional calls are blocked. (This setting is configured on the RLC for each site). This voice processing capacity defines how many calls can be active at one time.

The Remote Gateway 9150 unit ships with the ability to support up to 32 users, with up to 8 simultaneous calls (providing a 4:1 call blocking ratio). By adding additional DSP application or trunk interface modules, you can reduce or eliminate call blocking.

Reducing call blocking between the Remote Gateway 9150 unit and the host PBX

Each DSP application module provides the ability to support eight more simultaneous calls when voice traffic is routed over the IP network. Up to three more DSP application modules can be installed in the Remote Gateway 9150 unit, allowing 32 active calls at one time.

Note: If you add DSP capacity to the Remote Gateway 9150 unit, you must add the same DSP capacity to the RLC on the host PBX.

Trunks are required for the Remote Gateway 9150 unit to operate in PSTN mode (that is, over the PSTN instead of the IP network). Trunks are used to route calls between the Remote Gateway 9150 unit and the host PBX or the local PSTN.

By default, the Remote Gateway 9150 unit ships with no trunks installed. Trunks can be provided by installing trunk interface modules.

The number of trunks you can install depends on the type of trunk interface modules used on the Remote Gateway 9150 unit. For example, if ISDN BRI trunks are used, each trunk interface module provides one BRI trunk (providing two B-channels). You can install up to four trunk interface modules in the Remote Gateway 9150 unit.

Note: The Remote Gateway 9150 unit supports only ISDN BRI S/T or U trunks.

Calculating system requirements

To determine how many DSP application or trunk interface modules are needed to reduce or eliminate call blocking, use the “Remote Gateway 9150 System expansion worksheet” on page 385.

Administration PC

Install the Windows-based Remote Gateway 9150 administration software on a PC in the Remote Gateway 9100 Series network. This section describes options for connecting an administration PC to the Remote Gateway 9150 unit. It also describes the hardware and software requirements of the administration software.

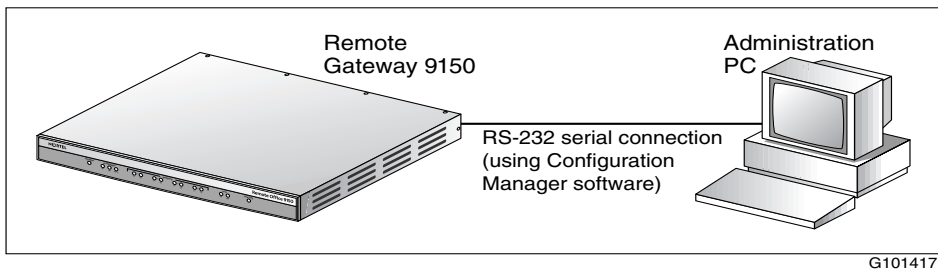
Connection options

The Remote Gateway 9150 product includes the Configuration Manager software that enables you to configure, administer, and upgrade the Remote Gateway 9150 unit. Perform these tasks over one of the following connections:

- RS-232 serial connection (required for first-time configuration only)
- 10BaseT Ethernet connection (for ongoing administration and upgrades)

Serial connection

Use the serial connection when you first install and configure the Remote Gateway 9150 unit. You must establish a serial connection to the Remote Gateway 9150 unit to enter the IP interface information. Refer to the following illustration:



You can continue using the serial connection for ongoing administration of the Remote Gateway 9150 unit, if you prefer. However, if this is the only connection option you use, you cannot administer the Remote Gateway 9150 unit remotely or perform upgrades.

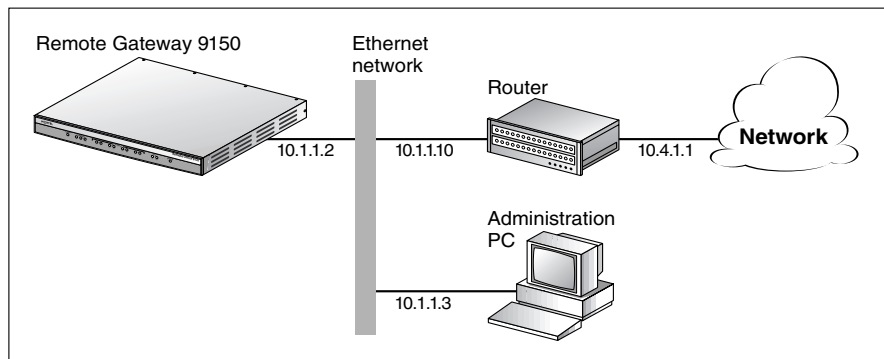
Note: When the administration PC is connected to the Remote Gateway 9150 unit through the serial port, you can view the command line interface using an application such as Telnet or HyperTerminal. However, the command line interface is not documented in this guide. Configuration Manager is the supported tool for administering the Remote Gateway 9150 unit over the serial port.

Ethernet connection

Once you configure the Remote Gateway 9150 unit with its IP interface information, the following can happen:

- Communication can be established between the Remote Gateway 9150 unit and the RLC (that is, calls can be routed over the IP network).
- You can administer and upgrade the Remote Gateway 9150 unit over the IP network.

This means you do not have to install an administration PC in the same location as the Remote Gateway 9150 unit. Refer to the following illustration:

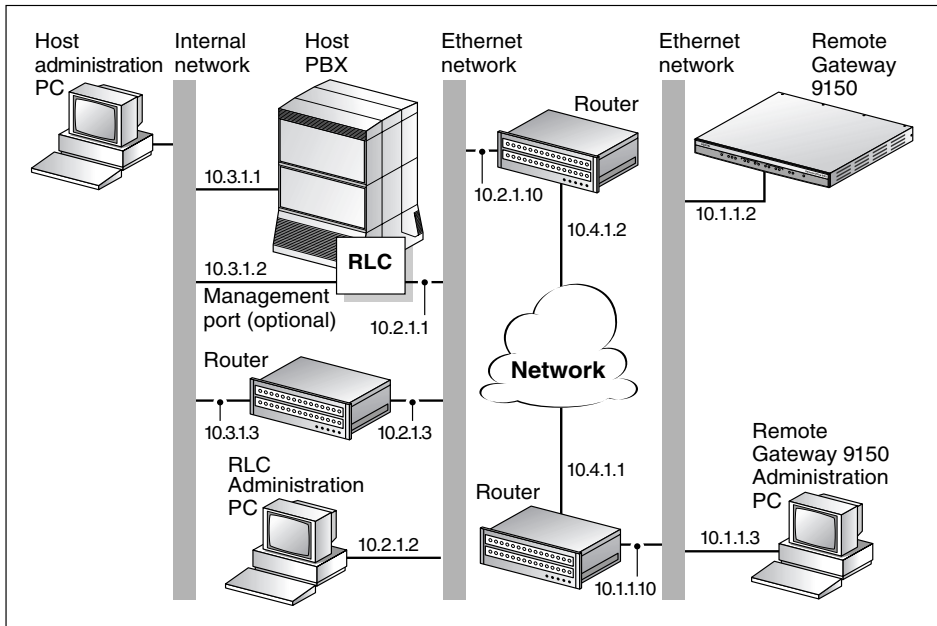


G101415

Administering multiple nodes in the network

If you are responsible for administering one or more Remote Gateway 9150 units and the RLC on the host PBX, you can access the Remote Gateway 9150 unit and the RLC from anywhere on the network. The following diagram shows an example of an assembled network with administration PCs.

Note: You do not have to install separate administration PCs for the RLC and the Remote Gateway 9150 unit. You can use one administration PC to administer all units in the Remote Gateway 9100 Series network.



Windows PC requirements

To use Configuration Manager, the administration PC must:

- be an IBM-compatible PC
- use a Windows 95, 98, NT Workstation 4.0, Millennium Edition (ME), 2000 Professional, or XP (Professional and Home Edition) operating system with the Microsoft TCP/IP networking component installed
- be equipped with a CD-ROM drive
- be equipped with a 10BaseT Ethernet interface card (this provides access to the Ethernet network)
- have an available COM port if you wish to use the RS-232 serial port to establish a direct serial connection
- be equipped with a pointing device, such as a mouse
- have 32 Mbytes of RAM for Windows 95, 98, and ME, or 64 Mbytes of RAM for Windows NT Workstation 4.0, 2000 Professional, and XP (Professional and Home Edition)
- have 48 Mbytes of available storage for Windows 95, 98 and ME, or 64 Mbytes of available storage for Windows NT Workstation 4.0, 2000 Professional, and XP (Professional and Home Edition)

Note: Configuration Manager does not support any of the Win32 Server versions of Microsoft Windows.

Trivial File Transfer Protocol (TFTP) server

Firmware upgrades and configuration uploads require that the administration PC have a TFTP server application installed. The administrator must know the TFTP server's IP address in the network. In other words, the IP address of the administration PC.

You can use any TFTP server application. These applications are available free of charge on the Internet.

Year 2000 compliance

The Remote Gateway 9150 unit and Configuration Manager software are Year 2000 compliant. However, ensure that the administration PC is Year 2000 compliant by verifying that the Windows operating system meets the compliance requirement listed in the following table:

Operating system	Year 2000 compliance requirement
Windows 95	Version 95b
Windows 98	OK as is
Windows NT Workstation 4.0	Service Pack 5 or higher
Windows 2000	Ok as is
Windows ME	Ok as is
Windows XP	OK as is

Optivity Telephony Manager and Configuration Manager

Nortel does not guarantee that Optivity Telephony Manager (OTM) and the Configuration Manager can operate simultaneously on the same administration PC. Simultaneous running of these two applications has not been tested and is, therefore, not supported.

Trunk connection management

You can manage trunk connections to the host PBX in several ways:

- Put the Remote Gateway 9150 unit into offline mode, so that it cannot place or receive calls through the host PBX when operating in PSTN mode.
- Define call duration and idle timers, if the trunk connection is defined as on-demand.
- Define minimum and maximum bandwidth allocation settings.
- Use QoS Transitioning Technology.

QoS Transitioning Technology

On IP networks, traffic congestion or delays can occur that result in poor voice quality or lost connections. The RLC can be configured to transition call processing from the IP network to the PSTN when the QoS degrades. When QoS on the IP network returns to normal, call processing can be transitioned back to the IP network.

The QoS thresholds (level and duration) defined on each RLC port determine when the transitions occur. To determine appropriate thresholds for each site in your network, consult your data network administrator. For more information, refer to the *Remote Gateway 9100 Series Network Engineering Guidelines* (555-8421-103).

Online/offline schedule

You can configure an online/offline schedule on the RLC to control when the Remote Gateway 9150 unit can place and receive calls through the host PBX. When the Remote Gateway 9150 unit is in offline mode, calls cannot be made or received through the host PBX over the IP or PSTN.

Configure offline entries:

- for times when the connection to the host PBX is not normally active, such as during evenings and weekends

- to prevent the Remote Gateway 9150 unit from staying online permanently, thereby eliminating unwanted ISDN BRI charges

When the RLC processes an offline entry, it instructs the Remote Gateway 9150 unit to go offline for a specified number of hours and minutes. The number of hours and minutes the Remote Gateway 9150 unit stays offline is the difference between the offline entry being processed and the next online entry.

For example, an offline entry is configured at 6:00 p.m. The next online entry is configured at 9:00 a.m. the following day. When the RLC processes the 6:00 p.m. entry, it instructs the Remote Gateway 9150 unit to go offline for 15 hours.

When going offline, a timer is activated within the Remote Gateway 9150 unit. When the timer expires (in the example above, at 9:00 a.m.), the Remote Gateway 9150 unit automatically initiates a “going online” request to the host PBX. If the RLC successfully receives the request, the Remote Gateway 9150 unit and its connected telephones go online.

Changing the online/offline mode

Whether an online/offline schedule is used or not, you can put the Remote Gateway 9150 unit into online or offline mode at any time by dialing the online or offline SPRE code at any telephone set connected to the Remote Gateway 9150 unit. The SPRE codes are configured on the Remote Gateway 9150 unit.

Trunk bandwidth allocation

The Remote Gateway 9150 unit can dynamically allocate available trunk bandwidth to active calls in PSTN mode. As calls are initiated and bandwidth requirements increase, additional trunk connections are established. Similarly, as calls terminate and bandwidth requirements drop, calls are aggregated and idle trunks are shut down.

Station configuration

When planning the stations at the Remote Gateway 9150 site, you must think about the call capabilities required by each station.

Each station at the Remote Gateway 9150 site inherits settings such as voice compression and priority from its associated RLC port. Configurations at the Remote Gateway 9150 site determine each station's ability to place locally controlled calls, host-controlled calls, or both. For stations defined with local control or local and host control, you can enable or disable specific features.

RLC settings

You must define the following on each RLC port:

- port allocation as dedicated, multi-user, or dynamic
- whether voice compression is used
- priority level

Port allocation

Assign each user at the Remote Gateway 9150 site to one port on the RLC on the host PBX. You can configure an RLC port in one of the following ways:

- as a dedicated port (one port per remote user)
- as a multi-user port (one port shared by multiple users)

Up to eight persons can share the same RLC port, but not at the same time. All stations that use this type of port must respond to the same DN and have identical telephone set configurations. This port type is especially useful for employees who are working in mutually exclusive shifts.

- as part of a dynamic pool

Dynamic port pooling is similar to a multi-user port except that the persons who share ports in a dynamic pool are assigned to the next available port in the RLC port pool. There is no correlation between the station and the port on the RLC.

This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

Voice compression

If calls are to be routed over the IP network, you must select one of the following voice compression algorithms on each RLC port:

- G.711: Voice is transmitted at 64 Kbps (no compression).
- G.726: Voice is compressed and transmitted at 32 Kbps.
- G.729A: Voice is compressed and transmitted at 8 Kbps.
G.729A is the default voice compression algorithm used by the RLC. This allows
 - up to six simultaneous voice calls to be processed over the first ISDN BRI B-channel (16 Kbps are reserved for signaling data)
 - up to eight simultaneous voice calls to be processed over the remaining ISDN BRI B-channels

Each Remote Gateway 9150 station inherits its compression algorithm from its assigned RLC port.

Station priority

You can configure each RLC port that is assigned to each station as normal priority, high priority, PSTN only, or IP only.

When the port is configured as high priority and the priority reserved setting is configured on the connection between the RLC and Remote Gateway 9150 unit, you can ensure voice QoS for calls to and from those stations.

For more details, refer to “Station priority” on page 36 and “Connection bandwidth” on page 37.

Notes:

1. Each Remote Gateway 9150 station inherits its priority setting from its assigned RLC port.
2. The number of RLC ports that you can configure as high priority depends on the amount of available bandwidth. The RLC administrator must ensure that enough bandwidth is available to process calls on normal priority ports.

Remote Gateway 9150 unit settings

You can define the following settings for each Remote Gateway 9150 station:

- port type as local, remote, or both
- extension (directory) number (on local stations only)
- key placement (on local stations only)

Port types

On the Remote Gateway 9150 unit, you can define each station with one of the following capabilities:

- local control only (local)
You can use stations defined as *local* to place and receive calls through the local PSTN. You can also place station-to-station calls at the Remote Gateway 9150 site. Calls through the host PBX are not allowed.
- host control only (remote)
If a particular station is not allowed to place or receive calls through the local PSTN, that station is configured as *remote* only. All calls are routed through the host PBX, except for emergency calls (such as 911). If the emergency service number is configured on the Remote Gateway 9150 unit, calls made to the emergency number are routed through the local PSTN so the emergency service receives the correct location information.
- both local and remote control
You can use stations defined as *local and remote* to place and receive calls through both the host PBX and the local PSTN. You can also place station-to-station calls at the Remote Gateway 9150 site.
Outgoing calls are routed according to the call appearance key used to initiate the call. Calls initiated on the key defined as the primary or host call appearance key are routed through the host PBX. Calls initiated on the key defined as the local call appearance key are routed through the local PSTN, if a trunk access code was dialed before the telephone number.

When a station is configured with local control capability, further configuration of the station is required to:

- enable or disable certain features
- disable outgoing calls or single-digit dialing, if required
- define key placement on the telephone

User extension configuration

Each station is assigned a local directory number (DN). The Remote Gateway 9150 unit uses the DN to route the incoming call to the correct station.

Stations that are configured with host-controlled call capability are associated with a port number on the RLC. The RLC and the Remote Gateway 9150 unit use this port number to establish the communication path between the host PBX and the station.

Placement of local call appearance and feature keys

When determining the placement of the local call appearance key on a station, ensure that the key position is not already configured for a specific feature on the host PBX. If you configure a PBX-configured feature key as a local call appearance key, the user cannot use that feature.

If the station is configured with local control capability, you can also configure the placement of other keys, such as Transfer, Call Waiting, and Make Set Busy.

Security

The RLC and Remote Gateway 9150 unit offer the following types of security:

- security level and, if required, security identifier to prevent toll fraud on the host PBX
- two levels of administration passwords to secure node configurations

Toll fraud

You can minimize toll fraud on the PBX by implementing one of the following levels of security:

- **Caller ID**
When Caller ID is selected, the Remote Gateway 9150 unit's calling line identification (CLID) is compared with its PSTN number configured on the RLC port when a connection to the host PBX is attempted. If they match, the connection is established. If they do not match, the host PBX drops the call.
Caller ID authentication cannot be performed over the IP network.
- **security identifier**
You can use security identifier authentication over the IP or PSTN. If you choose this level, you must configure a security identifier on both the Remote Gateway 9150 unit and its assigned RLC port. When an incoming call attempts to initiate a connection between the host PBX and Remote Gateway 9150 unit, Remote Gateway 9100 Series compares the security identifiers. If they match, the attempted connection succeeds. If they do not match, the host PBX drops the call and the connection fails.

Data network security

The Remote Gateway 9150 solution does not provide for data network security. If security on the data network is an issue, security must be implemented on the data network devices.

System configuration

The RLC and Remote Gateway 9150 unit configurations are protected by two layers of security:

- administration password

The administration password is required when starting the Configuration Manager software. If the password is not known, the person attempting to use the Configuration Manager cannot log on to any Remote Gateway 9100 Series node.

Note: A node is any RLC or remote site connected to the RLC.

- node password

The node password is required before the configuration of a particular node can be displayed or modified.

Planning for future growth

The Remote Gateway 9150 unit can change or grow along with your telecommunication needs. This section describes planning for accommodating those needs.

Adding DSP modules

The Remote Gateway 9150 unit ships with the ability to support up to 32 stations (you must assign all 32 to the same RLC). A Remote Gateway 9150 unit supports up to eight simultaneous voice calls when over the IP network.

You can increase the voice processing capability of the Remote Gateway 9150 unit by installing up to three more DSP modules. Each DSP module adds support for up to eight more simultaneous calls (to a maximum of 32).

To determine how many DSP application modules you need to install, use the “Remote Gateway 9150 System expansion worksheet” on page 385. For instructions on installing additional DSP modules, refer to “Installing trunk interface or DSP application modules” on page 93.

Refer to “DSP configuration” on page 239 for configuration information.

Note: When installing additional DSP modules on the Remote Gateway 9150 unit, you must also increase voice processing capability on the RLC. The number of modules that need to be added on the RLC depend on the requirements of other remote units connecting to the same RLC. If only this Remote Gateway 9150 unit is connecting to the RLC, then the same number of DSP modules must be installed on both the Remote Gateway 9150 unit and the RLC. To calculate the RLC’s DSP refer to the expansion worksheet in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Adding trunk interface modules

Initially, the Remote Gateway 9150 unit ships with no trunks. As connection needs change, you can add up to four ISDN BRI S/T or U trunk interface modules.

To determine how many trunk interface modules you need to install, use the “Remote Gateway 9150 System expansion worksheet” on page 385. For instructions on installing or replacing existing trunk interface modules, refer to “Installing trunk interface or DSP application modules” on page 93.

Maximum configurations

The following table identifies the maximum configurations for the Remote Gateway 9150 solution:

Component	Maximum
RLC connections	1
	Note: You must assign all users at the Remote Gateway 9150 site to the same RLC.
DSP application modules	3
ISDN BRI modules	4
ISDN BRI lines	4
	Note: Each line is associated with one ISDN BRI module and provides two B-channels.
Trunk groups	10
Digital telephones	32
Analog telephone or fax machine	1

Component	Maximum
MCAs or ATAs	<ul style="list-style-type: none">■ 4 if the Remote Gateway 9150 unit is connected to a 1-slot RLC (supporting 16 users).■ 7 if the Remote Gateway 9150 unit is connected to a 2-slot RLC (supporting 32 users). <p>Notes:</p> <ul style="list-style-type: none">■ You can have eight MCAs or ATAs installed if an analog telephone or fax machine is <i>not</i> installed.■ The total number of digital telephones and ATAs cannot exceed 32.

Deployment options

You can install and configure the RLC on the host PBX and Remote Gateway 9150 unit with the following network capabilities:

- only the IP network (Voice over IP)
- only the PSTN (for example, ISDN BRI trunks)
- both networks (required for QoS Transitioning Technology functionality)

If you choose not to use both networks initially, this section suggests how you can gradually phase in Voice over IP and QoS Transitioning Technology functionality.

ATTENTION!

Even if you plan to route calls over the PSTN only, you must assign an IP address and gateway to the Remote Gateway 9150 unit and RLC to allow remote administration.

Port and station assignment

Regardless of which network you use initially to route calls, you must plan RLC port and remote site user station assignments. Assign a single user at the Remote Gateway 9150 site to one RLC port that you configure on the host PBX with voice capability. This includes the analog port and the stations using ATAs.

Exception: You must assign stations that use MCAs for data transmission to ports that are configured on the host PBX with data capability.

If you plan to use the PSTN to route calls, one data port on the host PBX must be dedicated to the Remote Gateway 9150 site to establish the call connections.

Use the following forms to plan port and station assignment:

- “Remote Gateway 9150 Configuration Information—Stations” on page 376
- “Reach Line Card Connection Information—16 ports” planning form in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).
- “Reach Line Card Connection Information—32 ports” planning form in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Implementing PSTN mode

In a scenario involving the PSTN mode only, the PSTN processes all incoming and outgoing calls as follows:

IF the call is to or from the	THEN the call is in
host PBX,	host-controlled mode.
other PSTN customers,	locally controlled mode.

To implement PSTN mode, you must complete the following steps:

- 1 Determine how many simultaneous calls you want to process over the PSTN. This helps you determine how many trunk interface modules and DSP application modules to install on the Remote Gateway 9150 unit.

To do this, complete the “Remote Gateway 9150 System expansion worksheet” on page 385.

Similarly, you must calculate how many DSP application modules to install on the RLC (if any), using the “Reach Line Card System expansion worksheet” in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).
- 2 Arrange for ISDN BRI lines from the PSTN to the Remote Gateway 9150 site, if they are not already present.
- 3 Install ISDN BRI trunk interface and DSP application modules on the Remote Gateway 9150 unit, if needed. Up to four ISDN BRI modules and up to three DSP application modules can be installed.

Similarly, install DSP application modules on the RLC, if needed.

Note: The Remote Gateway 9150 unit does not ship with trunk interface modules or DSP application modules installed. The RLC does not ship with DSP application modules installed.

- 4 Obtain the ISDN BRI information for each line from the Remote Gateway 9150 site's PSTN service provider. This information must be configured on the Remote Gateway 9150 unit.
- 5 Identify the telephone number assigned to the B-channel that is to be the primary trunk connection to the RLC on the host PBX. This telephone number must be configured on the RLC, and is used by the RLC to establish connections with the Remote Gateway 9150 unit.
- 6 Similarly, obtain the telephone number assigned to this Remote Gateway 9150 unit's RLC port. This telephone number must be configured on the Remote Gateway 9150 unit, and is used by the Remote Gateway 9150 unit to establish connections with the RLC.

Implementing Voice over IP mode

In Voice over IP (VoIP) mode, the system processes all incoming and outgoing calls across the IP network through the host PBX. The system routes calls made to external parties to the PSTN using host PBX trunks. Calls processed through the host PBX are referred to as *host-controlled calls*.

Note: Local PSTN calls at Remote Gateway 9150 sites require access to ISDN BRI lines and the installation of ISDN BRI application modules in the Remote Gateway 9150 unit. All calls not routed through the host PBX, whether ISDN or POTS, are referred to as *locally controlled calls*.

To implement Voice over IP mode in host-controlled mode:

- 1 Determine how many simultaneous calls you want to process. This helps you determine how many DSP application modules to install on the Remote Gateway 9150 unit. To do this, complete the "Remote Gateway 9150 System expansion worksheet" on page 385.

Similarly, you must calculate how many DSP application modules to install on the RLC (if any), using the "Reach Line Card System expansion worksheet" in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

- 2 Install DSP application modules on the Remote Gateway 9150 unit, if needed. Up to three DSP application modules can be installed.
Similarly, install DSP application modules on the RLC, if needed.
- 3 Obtain an IP address assigned for the Remote Gateway 9150 unit. This IP address must be configured on the RLC, and is used by the RLC to establish connections with the Remote Gateway 9150 unit.
- 4 Similarly, obtain the IP address assigned to the RLC. This IP address must be configured on the Remote Gateway 9150 unit, and is used by the Remote Gateway 9150 unit to establish connections with the RLC.
- 5 Run this stage with a small number of users at first. Before applying VoIP mode to your entire remote network, you must ensure that one of the following is true:
 - Your IP network can handle the addition of remote network traffic.
 - You can identify the kinds of configuration adjustments you need to make to the IP network so that it can handle the additional traffic.

When you are satisfied with the IP network performance, continue with QoS Transitioning Technology implementation

Implementing Remote Gateway 9150 units behind Network Address Translation (NAT) routers

Some network routers run the NAT protocol to allow multiple devices in an Ethernet network to share the same broadband Ethernet address. An alternative to running the NAT protocol is to have the network administrator provide each device with its own broadband Ethernet address.

Remote Gateway 9150 units support NAT functionality. You can only connect a single Remote Gateway 9150 unit behind a NAT router. You can connect multiple Remote Gateway 9150 units behind a Network Address and Port Translation (NAPT) router. If you are not sure whether yours is a NAT router or a NAPT router, check with your vendor.

For a Remote Gateway 9150 unit connected behind a NAT or NAPT router you must:

- configure a permanent IP signaling connection
- assign a static IP address

Refer to “RLC connection configuration” on page 198 for the correct procedures.

Translation tables within NAT routers control the communication path from the private network to the public network. Most NAT devices contain timers that monitor the translation table entries. Each time the device uses a translation table entry, the timer restarts. Individual table entries are deleted if the communications path is not used and the timer expires.

It is possible, when using a Remote Gateway 9150 unit behind a NAT device, that prolonged periods of silence cause the NAT translation table entries to clear and drop the audio path. An example of this would be a remote user listening to a conference call with the user’s digital telephone set on mute. After five minutes (the default NAT translation table timer on many NAT routers) the remote user would not be able to hear the conference. To restore the NAT table entry and recover the audio path, the remote user could go off mute and speak into the digital telephone set.

To prevent the NAT translation table from dropping the audio path:

- configure the translation tables on the NAT router with a large timer value (for example, two hours)
- configure a static translation table entry for UDP port 20480

Implementing QoS Transitioning Technology

When the QoS Transitioning Technology is implemented, calls transition:

- to the PSTN when IP QoS degrades
- back to the IP network when IP QoS returns to normal

To implement QoS Transitioning Technology:

- 1 To implement the QoS Transitioning Technology, you must understand what your IP network is doing, such as
 - when the busy times are on the network
 - how much traffic is processed (during normal and busy traffic periods)
 - how to evaluate and adjust your network’s QoS

For more details, consult with your data network administrator and refer to the *Remote Gateway 9100 Series Network Engineering Guidelines* (555-8421-103).

- 2 Once you have this information and understand it, determine the appropriate QoS settings and configure them on each RLC port.
For instructions, refer to the Reach Line Card Installation and Administration Guide (NTP 555-8421-210).
- 3 If IP mode is the last stage in your network implementation, run this stage with a minimal number of users until you are sure that your IP network's QoS is acceptable.
- 4 When you are satisfied with QoS transitioning performance, deploy QoS Transitioning Technology to the rest of the network.

Planning the configuration

Before you configure the Remote Gateway 9150 unit, Nortel strongly recommends that you complete the data entry forms provided in Appendix A, “Planning forms.”

This section describes the information you can configure on the Remote Gateway 9150 unit.

Data entry form completion sequence

Complete the data entry forms in the following sequence:

1. Remote Gateway 9150 Configuration Information—Stations form
2. Remote Gateway 9150 Configuration Information—ISDN BRI Modules form
3. Remote Gateway 9150 Configuration Information—Network Connections form
4. Remote Gateway 9150 Configuration Information—Dialing Plans form

For more details, refer to Appendix A, “Planning forms.”

Station assignments and configuration

You must assign each telephone in your office to one of the 32 ports provided by the Remote Gateway 9150 unit. You can configure stations with the ability to place locally controlled calls (local), host-controlled calls (remote), or both (local and remote).

If you want a station to be able to place host-controlled calls, then map that station’s RLC port to telephone port configuration on the host PBX.

If you want a station to be able to place locally controlled calls, then you must take into consideration the numbering plan on the host PBX. Locally controlled calls include station-to-station calls. You must ensure that when users dial another station in the same office in host-controlled mode, the call routes correctly.

Stations used for locally controlled calls can be further configured with features and their key locations.

ISDN BRI information

To ensure that you get the correct ISDN service for the Remote Gateway 9150 unit, tell your service provider how you want the ISDN line to be provisioned. Request the following:

- two B-channels providing voice and data capability
Both B-channels must be Circuit Switched Voice and Data.
- Calling Line Identification (CLI) or Caller ID
CLI provides the caller's telephone number when you receive a call. This information is provided by the network and not the caller, so it can be used as a security measure to identify calls to be accepted and rejected.
- 64 Kbps clear channel
Note: A 64 Kbps clear channel is also required on the ISDN PRI connection between the host PBX and the PSTN. A 56 Kbps channel does not provide enough bandwidth to process one call using G.711 compression.

In return for providing the ordering information, your service provider gives you directory numbers and, if used in your area, Service Profile Identifiers (SPIDs). SPIDs are not provided for the AT&T 5ESS Custom service.

A directory number is the address or ISDN telephone number for the ISDN line assigned by the service provider. Each ISDN line receives at least one telephone number, called the Primary Directory Number.

If used in your area, your service provider provides you with the SPIDs. These are associated with the service you have ordered, and you must use these as part of the configuration for the Remote Gateway 9150 unit before any ISDN connections can be made (except for AT&T Custom). The SPID is similar to the ISDN telephone number and its format is unimportant as long as the information is entered correctly when configuring the Remote Gateway 9150 unit.

IP addresses

If you want to administer the Remote Gateway 9150 unit over the IP network, the following information is required for the Remote Gateway 9150 unit:

- IP address (it must be unique)
- subnet mask
- default gateway

If you want to route voice traffic over the IP network, you also need the RLC's IP address. The Remote Gateway 9150 unit uses these IP addresses to establish the connection with each other.

Connection link between the RLC and the Remote Gateway 9150 unit information

If you want to route voice traffic over the PSTN, the telephone numbers for each end of the network are required. If security is being implemented, the security authentication information (Caller ID or security identifier) is also needed.

Online/offline schedule

You can configure each port on the RLC with a schedule that identifies when a remote site is online (connected to the corporate PBX) or offline. When the Remote Gateway 9150 unit is in offline mode, calls cannot be made or received through the host PBX over the IP or PSTN.

You can configure only one online/offline schedule for the RLC port. This schedule affects all stations at the Remote Gateway 9150 site. Create offline entries:

- for times when the connection to the host PBX is not normally active, such as during evenings and weekends
- to prevent the Remote Gateway 9150 unit from staying online permanently, thereby eliminating unwanted ISDN BRI charges

To help you plan the online/offline schedule configuration on the RLC, use the "Reach Line Card Online/Offline Table Configuration" form in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Trunk configuration information

Trunk configuration on the Remote Gateway 9150 unit consists of defining the ISDN BRI lines from the central office and assigning one or more B-channels, if desired, to trunk groups.

Numbering plan

You must assign a trunk access code to each trunk group at the Remote Gateway 9150 unit site. A trunk access code is the number that must be dialed to obtain an outgoing trunk. In addition, you must define special prefix (SPRE) codes for the following features if you want to use them:

- paging
- to go online or offline (for more details, refer to “Online/offline table” on page 40)
- local calling
This allows analog or ATA-equipped station users to change the outgoing call mode to locally controlled mode. (Host-controlled mode is the default mode when users go offhook on analog or ATA-equipped stations.)
- registration and deregistration
The registration SPRE code is used to register the station user with a multi-user or dynamic port.
The deregistration SPRE code disengages the user from the port so that another user can use it. The user is put into *not logged in* mode.

All trunk access and SPRE codes are automatically defined in Configuration Manager with a pound sign (# in North America) so that there are no conflicts with host PBX dialing plans. The maximum length of each code is three digits in addition to the pound sign. For a list of the default SPRE and trunk access codes, refer to the “Remote Gateway 9150 Configuration Information—Dialing Plans” form on page 384.

Note: You can change the defaults if you prefer.

Chapter 3

Installing the Remote Gateway 9150 unit

In this chapter

General safety	86
Required installation tools	88
Unpacking and inspecting the equipment	89
Removing and replacing the Remote Gateway 9150 unit cover	90
Installing trunk interface or DSP application modules	93
Installing the Remote Gateway 9150 unit	98
Connecting the Remote Gateway 9150 unit	105
Powering up the Remote Gateway 9150 unit	111
Installing the Configuration Manager software	113
Using the Configuration Wizard to perform initial configuration	115
Testing the network connections	129

General safety

This section describes general safety guidelines recommended by Nortel, and tools needed for installation. Follow the safety guidelines and recommendations in this chapter whenever you perform installation or maintenance tasks on the Remote Gateway 9150 unit.



CAUTION

Risk of data loss or equipment damage

Electrostatic discharge (ESD) affects the performance and decreases the useful life of system components. It can seriously damage component parts, such as trunk interface and DSP application modules.

Implement the following precautions, as recommended by computer and telephone equipment manufacturers:

- Remove items that generate static charge from the installation site.
- Use antistatic spray if the site is carpeted.
- Ground yourself before handling any equipment. (For example, wear an antistatic wrist strap attached to any unpainted metal surface that is connected to an electrical ground.)

Precautionary messages

This guide provides warnings related to hardware installation and handling, such as the preceding caution. For a description of these warnings, refer to “Conventions used in this guide” on page xxii.

Safety precautions

To avoid damage or injury, follow these safety precautions at all times.

Plug the Remote Gateway 9150 unit into a properly grounded power source to reduce the possibility of electric shock and damage to the unit or network.



DANGER

Risk of electric shock

Disconnect the power as well as the Telco 1 and Telco 2 cables before you perform any hardware troubleshooting or add ISDN BRI or DSP application modules to the Remote Gateway 9150 unit.

If you do not disconnect the Telco 1 and Telco 2 cables from the Remote Gateway 9150 unit, you can receive a lethal shock if an external telco line is accidentally severed.

Ensure that nothing rests on connection cables, and that cables cannot be tripped over or stepped on.

Required installation tools

This section describes the tools necessary for Remote Gateway 9150 installation.

Required tools for hardware installation

You need the following tools to install the Remote Gateway 9150 unit, or to install or replace DSP application or trunk interface modules:

- antistatic ESD wrist strap (recommended)
- Phillips (cross-head) screwdriver
- pen or pencil for
 - noting the installation location (if mounting on a wall)
 - noting cable lengths
 - labeling cables
- cable tie wraps
- cable identification labels
- tape measure
- four wood screws if you want to mount the Remote Gateway 9150 unit on the wall

Required tools for software installation or upgrade

You need the following items for software installation or upgrade:

- *Remote Gateway 9100 Series Product CD-ROM*
- PC with a CD-ROM drive or an Internet connection for obtaining software, firmware, and documentation updates
- TFTP server application installed on the PC

The TFTP server is required for performing firmware upgrades. If a TFTP server is currently not installed, you can obtain one from the Internet.

Unpacking and inspecting the equipment

Before you unpack the equipment, ensure that your work area is safe from electrostatic discharge. For more details, refer to “Implement the following precautions, as recommended by computer and telephone equipment manufacturers:” on page 86. Before you install the Remote Gateway 9150 unit, ensure that the package contents are all present and are not damaged.

To inspect the package contents:

- 1 Inspect the Remote Gateway 9150 unit's shipping box for damage.
- 2 Open the box and remove its contents.
- 3 Verify that, in addition to this guide, the following items are present:



Item

- ☐ Remote Gateway 9150 unit
 - ☐ Package containing rubber feet and rack-mounting brackets with screws
 - ☐ Power cord and power supply
Note: In North America, the power cord and power supply are included inside the Remote Gateway 9150 box. In all other regions, the power supply is provided inside the box and the power cord for your region is provided outside the box.
 - ☐ RS-232 serial cable
 - ☐ *Remote Gateway 9100 Series and RLC Release Notes* (NTP 555-8421-102)
 - ☐ Remote Gateway 9100 Series Product CD-ROM
-

- 4 Visually inspect each item for obvious faults or damage.

If any component is damaged, report the damage immediately to your Nortel distributor and the carrier who delivered the equipment.

Removing and replacing the Remote Gateway 9150 unit cover

As you increase or change the voice processing capability of the Remote Gateway 9150 unit, you need to perform one or more of the following tasks:

- Install additional trunk interface modules.
- Install additional DSP application modules.

These tasks require you to remove the Remote Gateway 9150 unit cover.



DANGER

Risk of electric shock

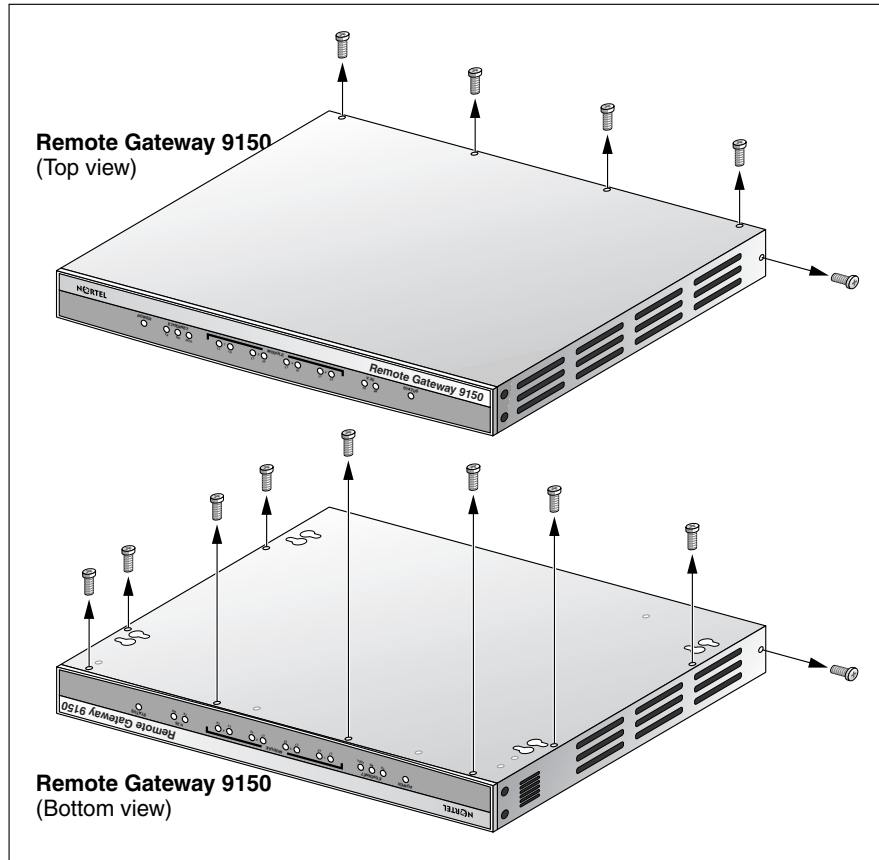
DISCONNECT THE POWER AS WELL AS THE TELCO 1 AND TELCO 2 CABLES BEFORE YOU PERFORM ANY HARDWARE TROUBLESHOOTING OR ADD ISDN BRI OR DSP APPLICATION MODULES TO THE REMOTE GATEWAY 9150 UNIT.

If you do not disconnect the Telco 1 and Telco 2 cables from the Remote Gateway 9150 unit, you can receive a lethal shock if an external telco line is accidentally severed.

To remove the Remote Gateway 9150 unit cover:

- 1 Use a Phillips screwdriver to remove the following screws from the Remote Gateway 9150 unit cover:
 - two screws from the sides
 - four screws from the top
 - eight screws from the bottom

Refer to the following diagram.



G101406

- 2 Place the screws in a safe place where they cannot be lost.
- 3 Ensure the Remote Gateway 9150 unit is placed top side up.
- 4 Remove the cover as follows:
 - a. Grasp both sides of the Remote Gateway 9150 unit.
 - b. Slide the cover toward you.
 - c. Lift the cover off the unit.
 - d. Put the cover aside.
- 5 Turn the Remote Gateway 9150 unit so the rear panel faces you.

Note: This allows you to read the labels on the Remote Gateway 9150 unit circuit board.
- 6 Perform module installation as required.

Note: For instructions, refer to “To install trunk interface or DSP application modules:” on page 96.
- 7 Replace the cover as follows:
 - Carefully slide the top cover into position over the circuit board so that the holes along the top edge of the rear panel are aligned.
 - Replace the four screws on the top.
 - Replace the two screws on the sides.
 - Turn the Remote Gateway 9150 unit over and replace the eight screws on the bottom.
- 8 Continue with “Installing the Remote Gateway 9150 unit” on page 98.

Installing trunk interface or DSP application modules

The Remote Gateway 9150 unit ships from Nortel with:

- no trunk interface modules installed
- one DSP built into the Remote Gateway 9150 unit's motherboard

Determining when to install trunk interface or DSP application modules

Perform the procedures in this section when you:

- need to expand the Remote Gateway 9150 unit's voice processing capability and have ordered additional modules (up to four trunk interface modules or three DSP application modules)
- need to replace a module because it is faulty

Before you can install a trunk interface or DSP application module, you must remove the cover from the Remote Gateway 9150 unit. For instructions, refer to "Removing and replacing the Remote Gateway 9150 unit cover" on page 90.

ATTENTION!

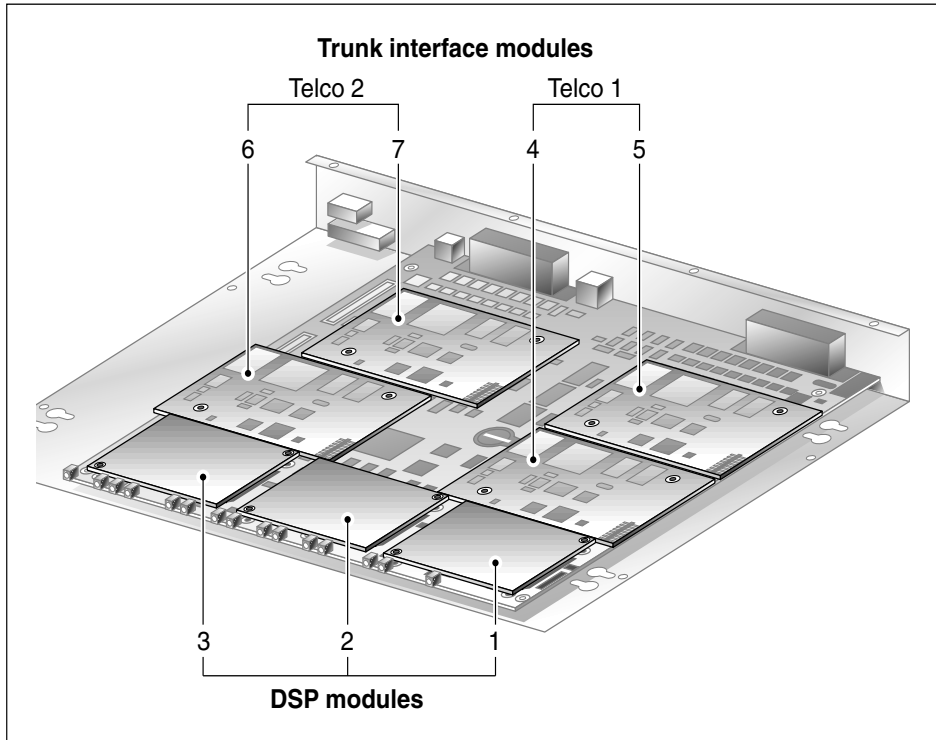
DSP application and trunk interface modules are sensitive pieces of electronic equipment and must be handled as such. Ensure that you follow the electrostatic discharge safety precautions described on page 86.

Determining where to install the modules

Each module position is labeled on the Remote Gateway 9150 unit circuit board as shown in the following table:

Module type	Valid module positions
DSP application module	<ul style="list-style-type: none">■ MOD 1■ MOD 2■ MOD 3
Trunk interface module	Telco 1 connector (phone lines 1 through 16): <ul style="list-style-type: none">■ MOD 4■ MOD 5
Trunk interface module (continued)	Telco 2 connector (phone lines 17 through 32): <ul style="list-style-type: none">■ MOD 6■ MOD 7 <p>Note: Each Telco connector provides access to two ISDN BRI lines (each with two B-channels).</p>

The following diagram shows where you can install the trunk interface and DSP application modules on the Remote Gateway 9150 unit circuit board:



G101408

Nortel recommends that you populate each module position in sequential order. Install trunk interface modules according to the Telco 1 or Telco 2 connections used.

Note: The Remote Gateway 9150 unit contains a dongle socket located in the middle of the circuit board. This dongle is not being used.

Installing trunk interface or DSP application modules

To install trunk interface or DSP application modules:

- 1 Clear a flat, static-free work area with sufficient space to hold your Remote Gateway 9150 unit and trunk interface or DSP application modules.
- 2 Place the trunk interface or DSP application modules in the work area.
Note: Keep the trunk interface or DSP application modules in their antistatic bags.
- 3 Remove a trunk interface or DSP application module from its antistatic bag.
- 4 Compare the connectors on the module with the connectors in the location where you want to install the module.

The connectors are keyed so that you can install a module in one way only. Ensure you hold the module so that the orientation of the connector keys match.

Refer to “Determining where to install the modules” on page 94, and the diagram on page 97.

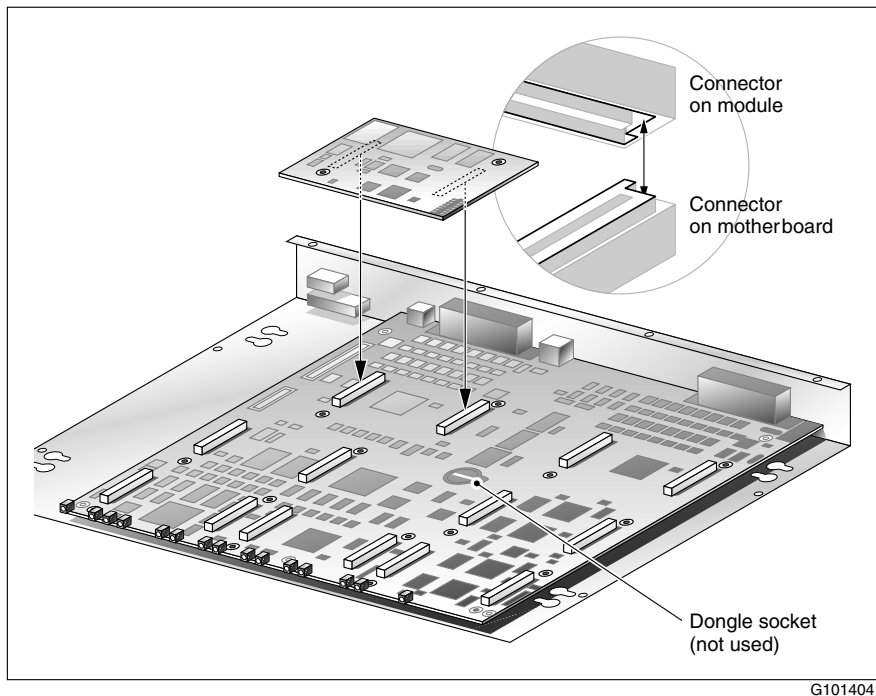
Removing trunk interface or DSP application modules

To remove trunk interface or DSP application modules:

Note: Perform this procedure only if you need to replace trunk interface or DSP application modules.

- 1 Use one hand to firmly grasp the long sides of the module that you want to remove.
- 2 Gently lift one side of the module up until it is free of the connectors on the Remote Gateway 9150 unit circuit board.
- 3 Lift the module up and away from the Remote Gateway 9150 unit circuit board, and place it to one side.

Note: If you are replacing this module, put it inside the replacement module’s antistatic bag for storage or to return it to Nortel for repair.



G101404

- 4 Align the connectors on the module with the connectors on the Remote Gateway 9150 unit circuit board.
- 5 Use both hands to grasp the module firmly and push down until it snaps into place.
- 6 Visually inspect the module connectors to ensure there is no gap between the module connectors and the Remote Gateway 9150 motherboard connectors.
- 7 Ensure that the module is securely installed by placing one finger beneath the module and tugging upward gently. When correctly installed, this action does not move the module.

Installing the Remote Gateway 9150 unit

You can install the Remote Gateway 9150 unit in the following locations:

- on a desk (refer to page 99)
- on a wall (refer to page 100)
- in a rack (refer to page 103)

The Remote Gateway 9150 unit package contains the following hardware:

- rubber feet for installing the Remote Gateway 9150 unit on a desk
- brackets with screws for installing the Remote Gateway 9150 unit in a rack

Note: If you want to mount the Remote Gateway 9150 unit on a wall, you must provide your own mounting hardware.

Choosing a suitable location

The Remote Gateway 9150 unit dimensions are:

- 42.5 cm (17 in.) wide (without rack-mounting brackets)
- 29.4 cm (11.75 in.) deep
- 4.4 cm (1.75 in.) high

For guidelines on where to install the Remote Gateway 9150 unit, refer to “Physical environment” on page 50.

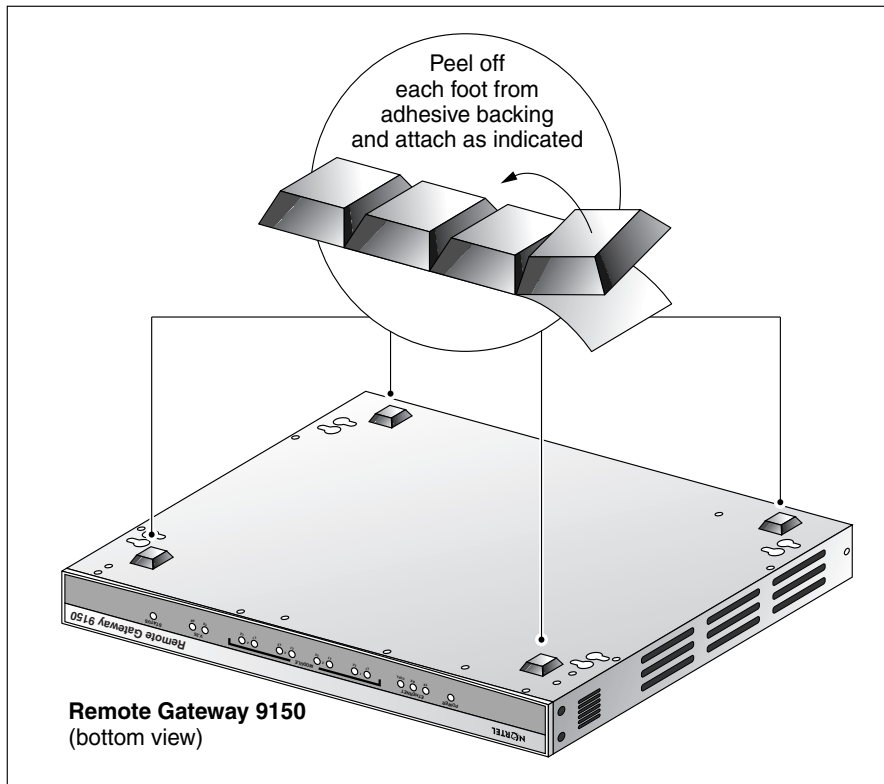
Note: Nortel recommends that you install the Remote Gateway 9150 unit in the same room as your communications equipment. Locate the Remote Gateway 9150 unit no farther than:

- 1230.7 m (4000 ft) from the digital telephones
- 307.7 m (1000 ft) from the analog device

Installing the Remote Gateway 9150 unit on a desk

To install the Remote Gateway 9150 unit on a desk:

- 1 Turn the Remote Gateway 9150 unit bottom side up.
- 2 Affix the rubber feet to the Remote Gateway 9150 unit as shown in the following diagram:



G101395

- 3 Ensure the rubber feet are securely fastened.
- 4 Place the Remote Gateway 9150 unit in the desired location.
- 5 Continue with "Connecting the Remote Gateway 9150 unit" on page 105.

Installing the Remote Gateway 9150 unit on the wall

To install the Remote Gateway 9150 unit on the wall:

Do not affix the rubber feet to the bottom of the Remote Gateway 9150 unit. Otherwise, the unit cannot be mounted flush against the wall.

To mount the Remote Gateway 9150 unit on the wall, you must provide your own screws. You need suitable size screws that are long enough to ensure the Remote Gateway 9150 unit is securely mounted.

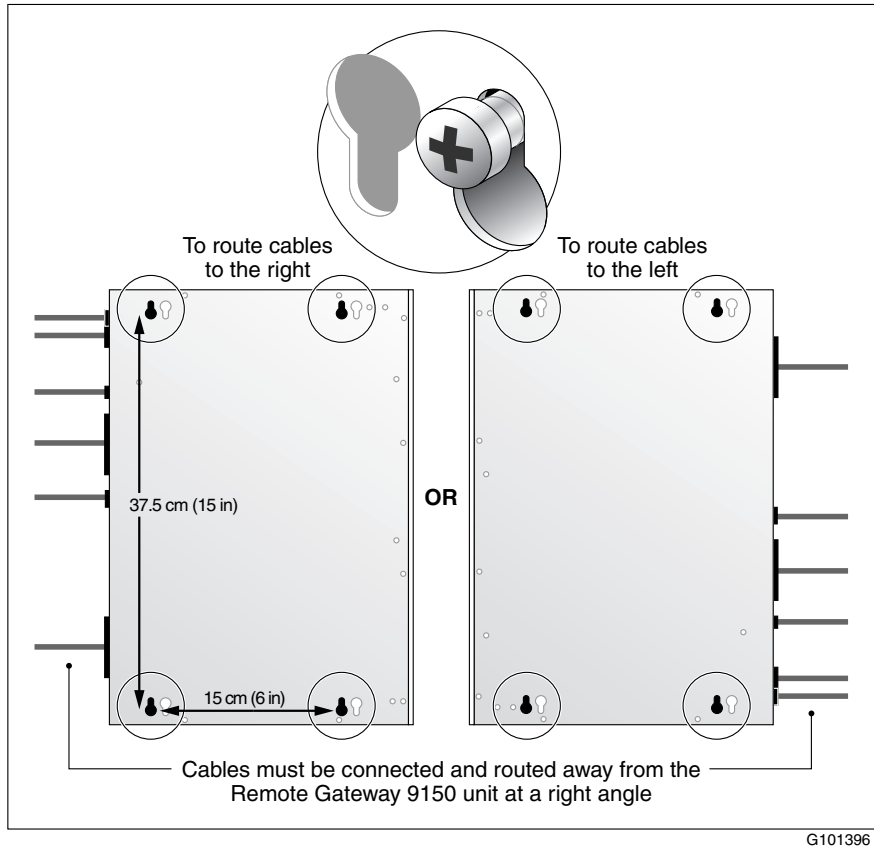
When mounting the Remote Gateway 9150 unit on the wall, you must use standard telephony installation practices. The unit must be mounted so that:

- the cables are at right angles to the unit
- the rear (connection) panel faces left or right

Ensure that:

- the LED indicators on the front panel can be viewed easily
- the chosen location provides enough space to accommodate the cables when they are connected to the Remote Gateway 9150 unit

Refer to the diagram on page 101.



- 1 Choose the location on the wall where you want to mount the Remote Gateway 9150 unit.

- 2 Use the pre-drilled screw slots on the bottom of the Remote Gateway 9150 unit as a guide to measure and mark the location on the wall for each mounting screw.

The measurements between the screw slots are as follows:

- from front to back panels: 15 cm (6 in.)
- from side to side: 37.5 cm (15 in.)

Note: Two sets of screw slots are provided. Each set allows you to route the cables to the left or right when the Remote Gateway 9150 unit is correctly mounted. Ensure you use the same screw slot orientation for each location that you mark on the wall.

- 3 Mount the screws.

Note: Do not screw the screws all the way in. Screw the heads to about 5 mm (1/8 in.) from the wall.

- 4 Mount the Remote Gateway 9150 unit on the screws, and then gently pull it down so the screws slide into the narrow portion of the screw slots.

Do not let go yet!

- 5 Ensure the Remote Gateway 9150 unit is securely mounted.



WARNING

Risk of personal injury or equipment damage

Ensure the Remote Gateway 9150 unit is securely fastened to the wall. Otherwise, it can fall, be damaged, and cause injury to yourself or others.

- 6 When you are satisfied that the Remote Gateway 9150 unit is securely mounted, continue with “Connecting the Remote Gateway 9150 unit” on page 105.

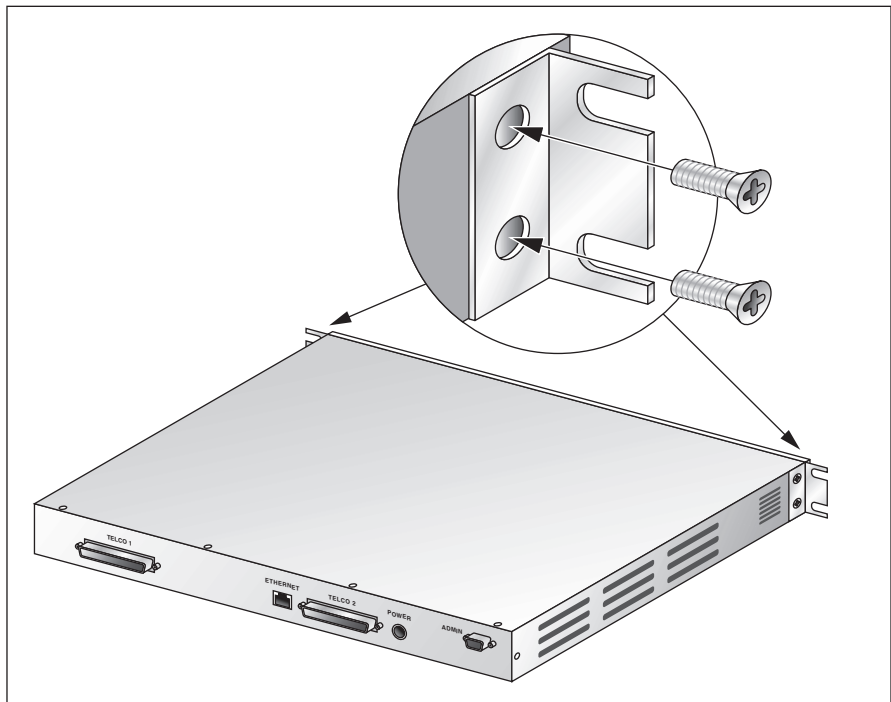
Installing the Remote Gateway 9150 unit in a rack

The rack slot chosen for the Remote Gateway 9150 unit must:

- be large enough to provide air circulation to keep the Remote Gateway 9150 unit cool
- allow you to securely fasten the Remote Gateway 9150 unit to the rack using the rack-mount brackets

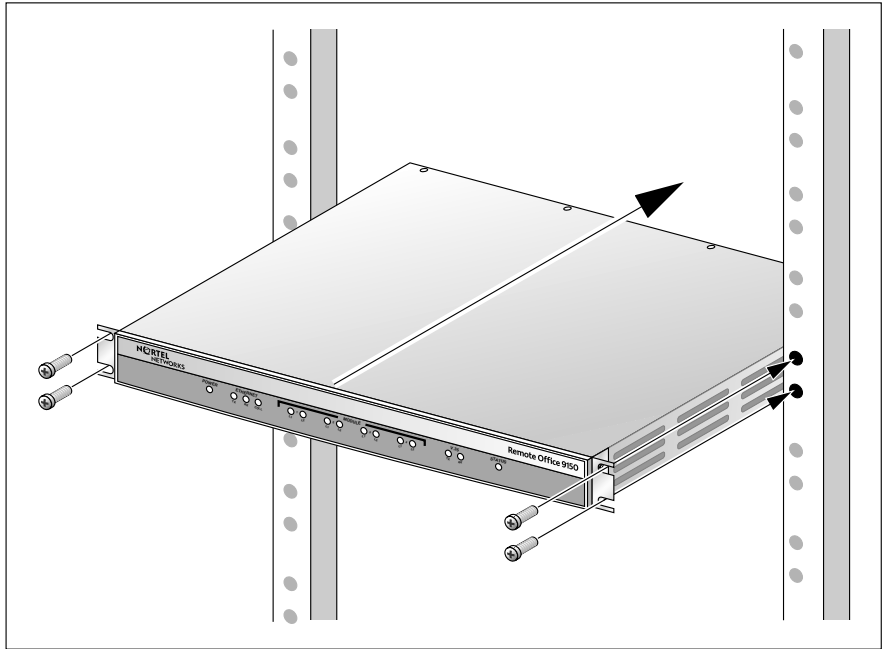
To install the Remote Gateway 9150 unit in a rack:

- 1 Attach the rack-mount brackets as shown in the following illustration.



G101537

- 2 Slide the Remote Gateway 9150 unit into the rack slot.



G101398

- 3 Secure the Remote Gateway 9150 unit to the rack with nuts and bolts.
- 4 Continue with "Connecting the Remote Gateway 9150 unit" on page 105 when you are satisfied that the Remote Gateway 9150 unit is securely installed.

Connecting the Remote Gateway 9150 unit

When you establish the cabling connections, you are connecting the Remote Gateway 9150 unit to the:

- power source
- telephones and ISDN BRI trunks

Note: If you are connecting the Remote Gateway 9150 unit to a Meridian 1 PBX in-building cross-connect system, you need a QCBIX1A BIX block.

- Ethernet network
- administration PC

Cables you must provide

Ensure that you have obtained the telephone and Ethernet cables for your network. These cables are not supplied in the Remote Gateway 9150 unit package.

The cables must meet the following requirements:

- telephone cable: One end of the cable must provide a male 50-pin connector. (This end connects to the Remote Gateway 9150 unit.)
Ensure the other end of the cable matches the connectors needed to connect to the telephones or trunks. (For example, if you are using a BIX block to establish the telephone connections, the wires inside must be exposed.)

Notes:

- Two telephone cables are required, depending on how many telephones and trunks are installed. (Each telephone cable provides support for up to 16 digital telephones and two ISDN BRI lines providing two B-channels each. The Telco 1 cable also provides support for one analog station such as a fax machine.)

Nortel recommends that you use straight-through Amphenol cables instead of side-entry Amphenol cables. (Refer to “Attaching the cables to Remote Gateway 9150 unit” on page 108.)

- Digital telephones must be located no farther than 1230.7 meters (4000 feet) from the Remote Gateway 9150 unit.

- The analog device must be located no farther than 307.7 meters (1000 feet) from the Remote Gateway 9150 unit.
- Ethernet cable
If you are connecting the Remote Gateway 9150 unit to a hub, you need a standard CAT5 un-shielded twisted-pair (UTP) straight-through Ethernet cable. The cable must be no longer than 100 meters (325 feet) in length.

Connector and pin-out reference

The following table identifies where to find the pin-out table for each connector:

Connector	Connection type	For the pin-out table, refer to
TELCO 1	25 TIP and RING pairs	page 404.
TELCO 2	25 TIP and RING pairs	page 406.
ETHERNET	RJ-45	page 408.
ADMIN	DB-9	page 409.
Power	DIN	page 410.

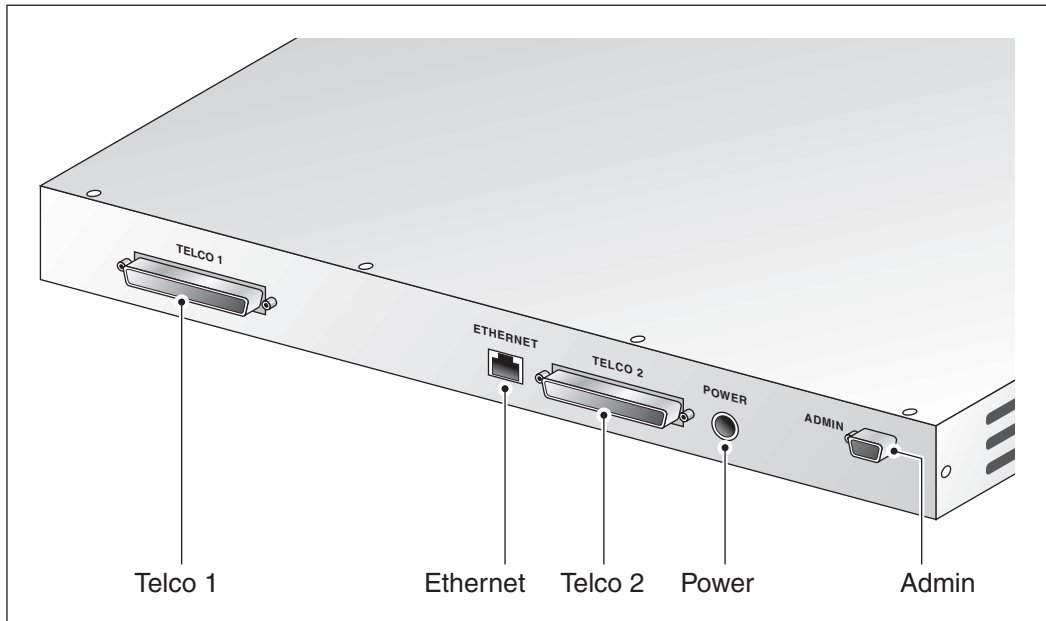
More information

The following documents describe how to establish telephone and trunk connections using the Meridian 1 PBX BIX in-building cross-connect system:

- *Meridian 1 PBX Installation planning* (NTP 553-3001-120)
- *Telephone and attendant console installation* (NTP 553-3001-215)
- *BIX* In-Building Cross-Connect System Material Installation and Servicing (Wall-Mounted System)* (NTP 631-4511-200)

Remote Gateway 9150 unit connection panel

The following diagram shows the connectors on the back panel of the Remote Gateway 9150 unit:

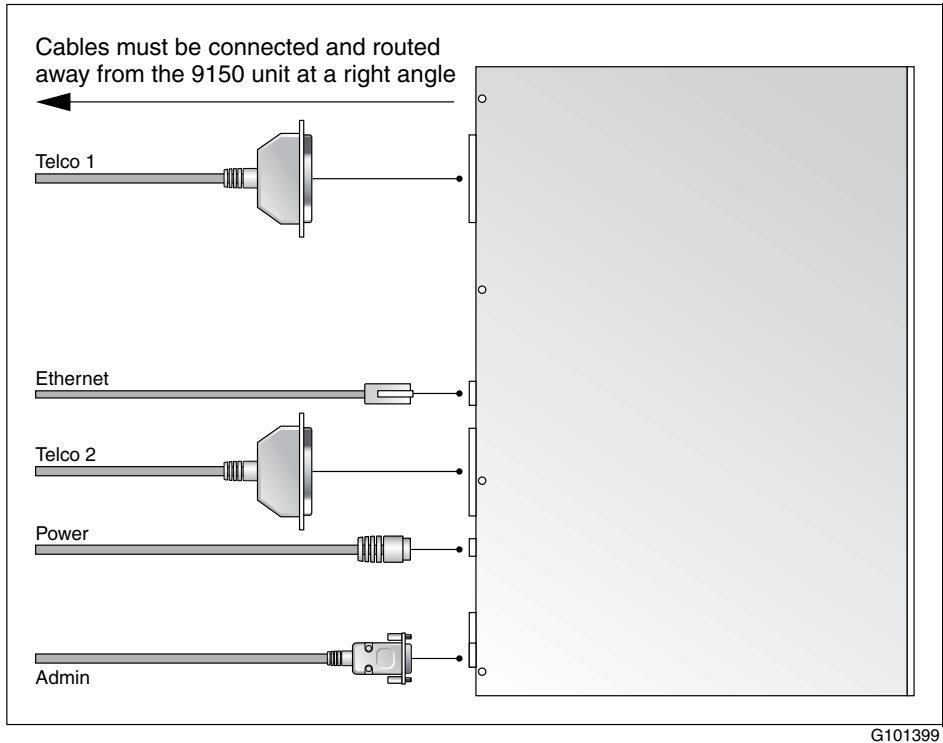


G101535

Note: If you want to connect the Remote Gateway 9150 unit to an uninterruptible power supply (UPS), ensure the UPS has a minimum of 100 Watts available.

Attaching the cables to Remote Gateway 9150 unit

Nortel recommends that you use straight-through Amphenol cables instead of side-entry Amphenol cables, as shown in the following diagram:



Note: The Remote Gateway 9150 Telco 1 and 2 connections provide the opposite gender of the connections on Meridian 1 PBX IPE or Meridian 1 PBX 11 cabinet line card slots. Therefore, you must use different cables when connecting to the Remote Gateway 9150 unit than the cables you use to connect to Meridian 1 PBX line cards.

Connecting the Remote Gateway 9150 unit to the network



WARNING

Risk of electric shock or damage to equipment

To reduce the risk of electric shock to yourself or damage to the Remote Gateway 9150 unit, ensure that the power source to the unit is turned off until the Telco 1 and Telco 2 connections have been completed.

To connect the Remote Gateway 9150 unit to the network:

- 1 Connect the male 50-pin connector of the telephone cable to the TELCO 1 connector on the Remote Gateway 9150 unit.

Secure the cable connection by snapping the wire tabs into place or by inserting screws.
- 2 Establish the connections to the telephones and trunks according to the pin-out table in “TELCO 1 connector pin-out table” on page 404 (in Appendix C).
- 3 Connect the Remote Gateway 9150 unit to the Ethernet network if you want to route calls over the IP network, or administer the Remote Gateway 9150 unit from another location, by doing the following:
 - a. Connect one end of the RJ-45 Ethernet cable to the ETHERNET connector on the Remote Gateway 9150 unit.
 - b. Connect the other end to an Ethernet hub.
- 4 Connect the male 50-pin connector of the other telephone cable to the TELCO 2 connector on the Remote Gateway 9150 unit.

Note: Secure the cable connection by snapping the wire tabs into place or by inserting screws.
- 5 Establish the connections to the telephones and trunks according to the pin-out table in “TELCO 2 connector pin-out table” on page 406 (in Appendix C).

- 6 Connect the ADMIN connector on the Remote Gateway 9150 unit to the administration PC as follows:
 - a. Connect the male 9-pin connector of the supplied RS-232 serial cable to the ADMIN connector on the Remote Gateway 9150 unit.
Note: You may need to provide an RS-232 adapter if the available RS-232 port on your PC does not match the connector on the serial cable.
 - b. Connect the other end to an available COM port on the PC.
- 7 Connect the Remote Gateway 9150 unit to the power source as follows:
 - a. Connect the four-pin plug on the power transformer to the POWER connector on the Remote Gateway 9150 unit.
Note: Ensure the arrow on the four-pin plug faces up.
 - b. Connect the AC cord to the AC power receptacle on the power transformer.
 - c. Plug the AC cord into a 110 V or 220 V uninterruptible power source (UPS) or wall outlet.
- 8 Proceed with “Powering up the Remote Gateway 9150 unit” on page 111.

Powering up the Remote Gateway 9150 unit

As soon as you connect the Remote Gateway 9150 unit to the power source, the unit begins to power up.

Note: If you are connecting a Remote Gateway 9150 unit to a UPS (uninterruptible power supply), ensure that the UPS has a minimum of 100 Watts available.

During power up, the following events occur:

- The Remote Gateway 9150 unit performs a self-test that verifies all critical functionality.
- An LED indicator test sequence is performed.

Power-up self-test

During power-up, the Remote Gateway 9150 unit performs a self-test that verifies all critical functionality, including:

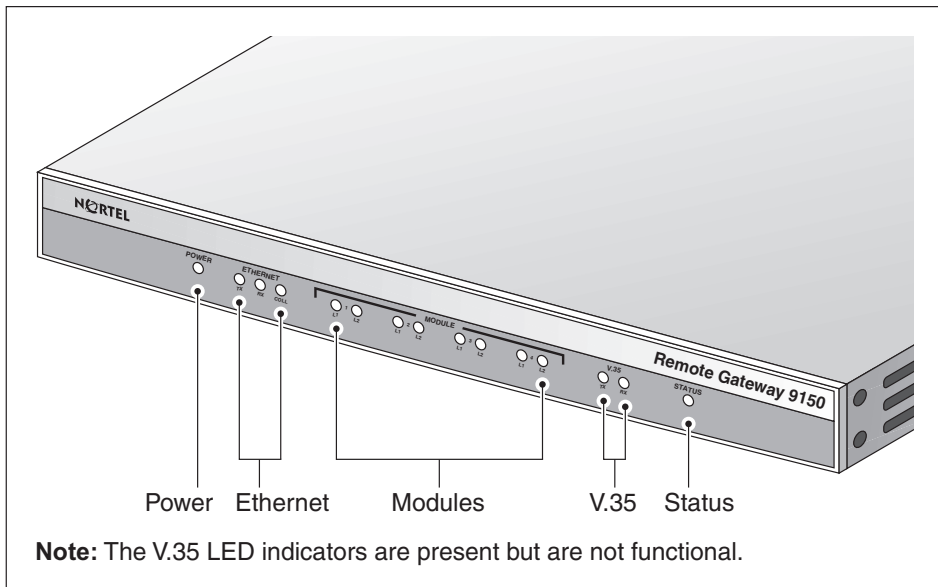
- RAM memory test
- EPROM checksum validation
- Flash checksum validation
- DSP health
- interface loopbacks

The power-up cycle also automatically detects if one or more trunk interface or DSP application modules have been installed. You can configure trunk interface and DSP application modules using Configuration Manager.

The power-up cycle takes about 60 seconds to complete.

LED indicator test sequence

The following diagram shows the LED indicators on the front panel:



G101402

During the power-up cycle, the LED indicators behave as follows:

1. All LED indicators light for about 15 seconds.
2. The Module LED indicators light individually in sequence (1 through 8).
3. All LED indicators light.
4. All LED indicators except the Status LED go out. The Status LED remains lit.

Note: Steps 2 through 4 take about 4 to 5 seconds.

After this point, the Remote Gateway 9150 unit is functional.

Notes:

- The ETHERNET TX and RX and module (ISDN BRI) LED indicators flash only when transmit and receive activity is present on those interfaces.
- The ETHERNET COLL LED indicator flashes when a data collision occurs on the line.

Installing the Configuration Manager software

Use the Configuration Manager software to configure and administer the Remote Gateway 9150 unit. This software is located on the CD-ROM provided in the package. You must install this software on the administration PC to configure and administer the Remote Gateway 9150 unit and the Remote Gateway 9100 Series system.

Note: Leave DLL files installed by the Configuration Manager InstallShield in the Windows system directory. Do not move these files to any other directory.

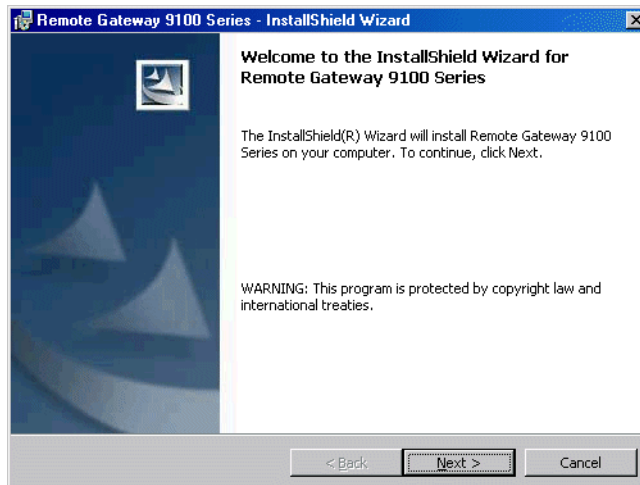
To install the software:

- 1 Insert the CD-ROM in the applicable drive on your PC.

Result: If autorun is enabled on your PC, a Welcome screen displays listing available options.

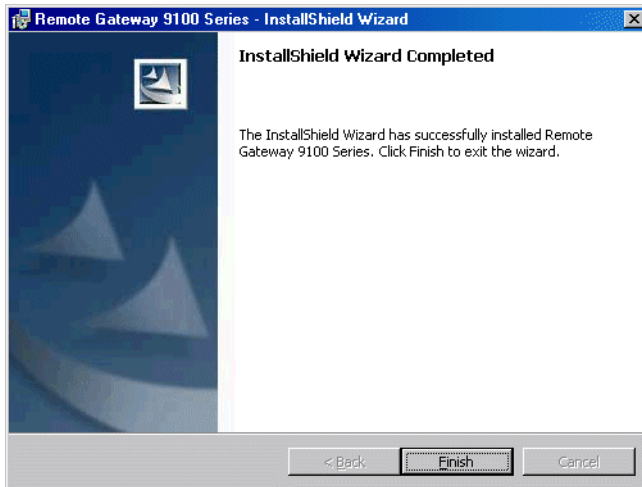
- 2 If autorun has started, select the Install option; otherwise, navigate to the software directory, and then locate and double-click on the setup.exe icon.

Result: The InstallShield Wizard prepares for installation, and then the Welcome screen displays, similar to the following:



- 3 Click on the **Next** button, and then follow the screen prompts.

Result: Once the software has been installed successfully, the InstallShield Wizard Completed screen displays, similar to the following:



- 4 Click on the **Finish** button.

Result: The InstallShield closes.

Using the Configuration Wizard to perform initial configuration

The Configuration Wizard option in Configuration Manager allows you to configure the minimum information needed for establishing communications between the Remote Gateway 9150 unit and the RLC at the host site. The Configuration Wizard does not provide all the configuration settings that are available in Configuration Manager. By using the Configuration Wizard, the Remote Gateway 9150 unit can be up and running within 10 minutes.

You can use the Configuration Wizard in offline mode or while connected and logged on to the Remote Gateway 9150 unit (online mode).

What you can configure with the Configuration Wizard

The Configuration Wizard allows you to configure the following:

- the Remote Gateway 9150 unit's IP address, subnet mask, and default gateway

This information must be valid for your IP network.

Note: If you are not planning to use the IP network to route calls, you must enter this information for administrative purposes. If you do not have an IP network in place, use the sample information provided on page 119.

- for Voice over IP capability: the IP address for the RLC at the host site
- for PSTN capability:
 - the telephone number of the RLC at the host site
 - information provided by your ISDN service provider for each ISDN BRI trunk interface module (telephone numbers, SPIDs, and switch type)

Ensure you have this information ready before you begin.

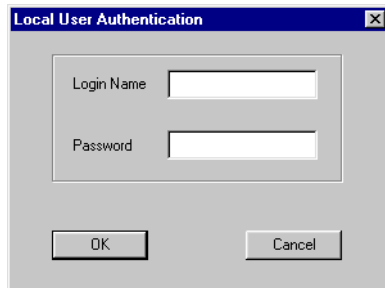
Note: If, after completing configuration with the Configuration Wizard, you want to modify any settings, you must use Configuration Manager.

Starting Configuration Manager

To start Configuration Manager:

- 1 Click on Start → Programs → Remote Gateway 9100 Series → Configuration Manager.

Result: Configuration Manager opens and displays the Local User Authentication dialog box, similar to the following, prompting you for the login name and password:



- 2 Enter **admin** into the Login Name field.
- 3 Enter **root** into the Password field.
- 4 Click on the **OK** button.

Result: The Configuration Manager dialog box displays informing you of a successful log on.



- 5 Click on the **OK** button.

Result: The Configuration Manager dialog box closes.

- 6 Do one of the following:

IF you want to perform an

THEN

offline configuration,

a Choose View → Device Type → 9150.

b Continue with “Performing configuration with the Configuration Wizard” on page 119.

online configuration,

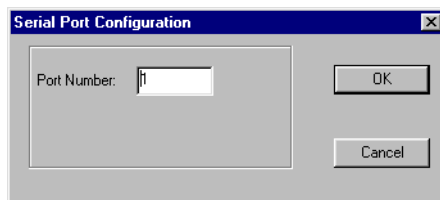
continue with “Establishing a serial connection” below.

Establishing a serial connection

To establish a serial connection:

- 1 From the Menu Bar, choose Connect → Logon Unit → Serial.

Result: The Serial Port Configuration dialog box displays, similar to the following:



- 2 Enter the Remote Gateway 9150 unit's associated COM port, and then click on the **OK** button.

Result: The User Authentication for Serial Mode dialog box displays, similar to the following:

- 3 Enter **guest** in the Login Name field.
4 Enter the default password, **guest123**, in the Password field.

Note: Nortel recommends that you do not change the password until your system is up and running.

- 5 Click on the **OK** button.

Result: Configuration Manager initiates a connection attempt and displays the following message:

Trying Connection

IF the logon attempt THEN

fails,

the following message displays:

10060 SERIAL CONNECTION FAILED

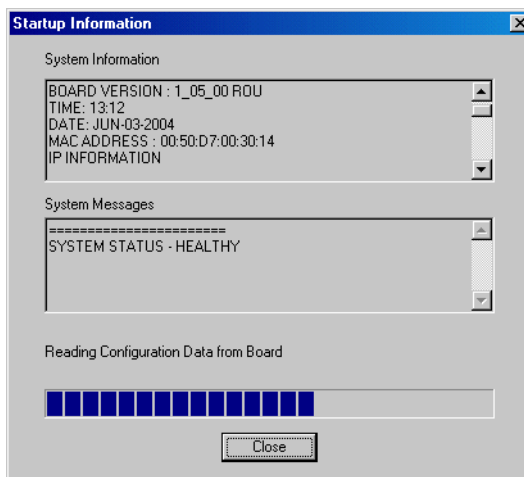
Check the serial connection and ensure it is good. Then, go back to step 1.

is successful,

the User Logged In dialog box displays.

Click on the **OK** button.

Result: The Startup Information dialog box displays, similar to the following:



IF the logon attempt THEN

successful,
(continued)

The following messages, similar to the following, display above the progress bar at the bottom of the dialog box:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages indicate that Configuration Manager is obtaining the unit's configuration information from Flash memory.

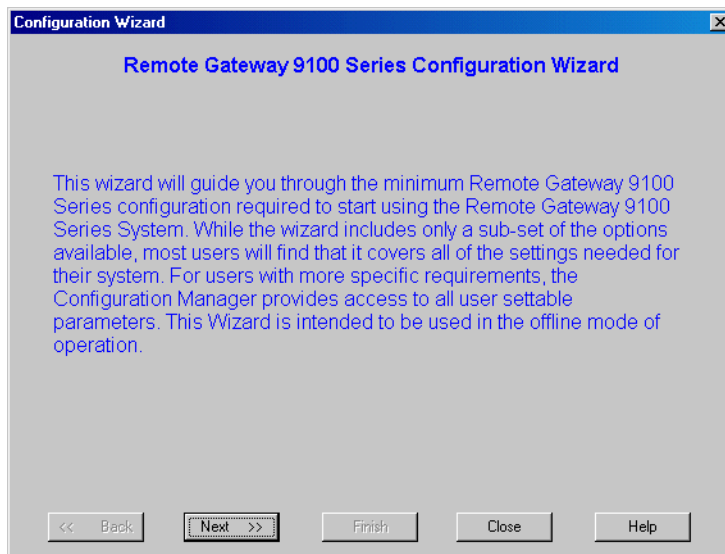
Click on the **Close** button.

Performing configuration with the Configuration Wizard

To perform configuration with the Configuration Wizard:

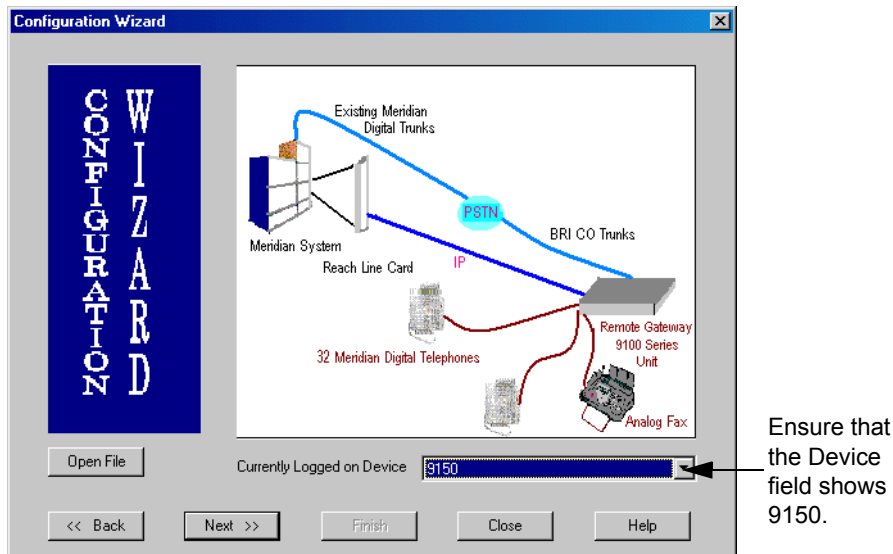
- 1 From the Menu Bar, choose Configuration Wizard.

Result: The Configuration Wizard screen displays, similar to the following:



- 2 After reviewing the message, click on the **Next** button.

Result: The Configuration Wizard screen displays, similar to the following:



- 3 Verify that the Currently Logged in Device drop down box shows 9150. If it does not show 9150, select 9150 from the drop down list.
- 4 Click on the **Next** button.

Result: The Local Unit Configuration dialog box displays. A completed example is shown on page 122.

- 5 Complete the fields on this dialog box as described in the following table:

Field	Description
Set the unique Unit ID of the unit	Enter the number from 1–255 that uniquely identifies the Remote Gateway 9150 unit you are configuring for a particular RLC. Note: Each unit connected to a RLC must be given a unique unit ID. This implies that Remote Gateway 9150 units that connect to different RLCs in the network can have the same unit ID.

Field	Description
Enter a node name that identifies the unit	Enter a name that uniquely identifies the Remote Gateway 9150 unit you are configuring.
Enter the local IP Address of the unit	Enter the IP address assigned to the Remote Gateway 9150 unit. Note: If you do not have a valid IP address, enter the sample IP address: 10.1.1.2.
Enter the Local IP Mask of the unit	Enter the subnet mask. Note: If you do not have a valid subnet mask, enter the sample subnet mask: 255.255.0.0.
Enter the Local IP Gateway of the unit	Enter the IP address of the gateway between the Remote Gateway 9150 unit and the network. Note: If there is no router between the Remote Gateway 9150 unit and the network, then the administration PC acts as the gateway. Enter 10.1.1.10 : <ul style="list-style-type: none">■ as the IP address on the administration PC■ as the gateway on the Remote Gateway 9150 unit

The following is a completed example:

The IP information allows you to administer the Remote Gateway 9150 unit from any location on the network.

- 6 Click on the **Next** button.

Result: The Set the Configuration for the Remote Unit dialog box displays. A completed example is shown on page 124.

- 7 Complete the fields on this dialog box as described in the following table:

Field	Description
Set the Unit ID of the RLC to connect to	Enter the RLC's unit ID.
Wish to Enable IP Voice Connection to Remote	<ul style="list-style-type: none"> ■ Click on the Yes option button to enable the Voice over IP connection to the RLC. Then enter the RLC's 32-bit, decimal dot notation address (xxx.xxx.xxx.xxx). This is not the URL's site name that begins www. ■ Click on the No option button to disable the Voice over IP connection to the RLC. Clicking on the No option button dims the IP Address fields.

Field	Description
Wish to Enable PSTN Connection to Remote	<ul style="list-style-type: none"> ■ Click on the Yes option button to enable the PSTN connection to the RLC. Then enter the telephone number that must be dialed to connect to the RLC. The telephone number can include the following digits or characters: 0 through 9, #, *, comma (,), period (.), and dash (-). <ul style="list-style-type: none"> ■ Caller ID separator: “.” (period) ■ Caller ID separator and 1/2 second delay: “,” (comma) ■ null separator: “-” (dash) ■ Click on the No option button to disable the PSTN connection to the RLC. Clicking on the No option button dims the PSTN Number fields.
Wish to configure Multiple 9150 Ports	<ul style="list-style-type: none"> ■ Click on the Yes option button if you want to assign Remote Gateway 9150 ports to digital telephones now. Then, do the following: <ul style="list-style-type: none"> ■ Enter the first RLC port number to assign. Note: Nortel recommends that ports be configured so that the RLC port number matches the Remote Gateway 9150 unit’s port number. ■ Enter the number of telephones connected to the Remote Gateway 9150 unit. ■ Click on the No option button if you want to complete port assignment at a later time with Configuration Manager.

The following is a completed example:

Click on the **Yes** option button to allow voice calls over IP, then enter the RLC's IP address.

Click on the **Yes** option button to allow voice calls over the PSTN, then enter the RLC's phone number.

Click on the **Yes** option button to automatically assign Remote Gateway 9150 unit ports to RLC ports, then enter the information as described previously.

- 8 Click on the **Next** button.

Result: The Enter the BRI module data dialog box displays. A completed example is shown on page 125.

- 9 Complete the fields on this dialog box as described in the following table:

Field	Description
Which module would you wish to configure	Click on the option button immediately to the left of the number of the trunk interface module that you are configuring. The number you select must match the position where the module has been installed in the Remote Gateway 9150 unit.
Module Status	This field identifies whether a module has been physically installed on the Remote Gateway 9150 unit.

Field	Description
Select the Switch Type	Select the type of switch used by your ISDN service provider.
Select the ISDN Line Type	Select the ISDN variant used in your country.
Enter the PSTN Number (B channel 1 and B channel 2)	Enter the telephone number provided by your ISDN service provider for this B-channel.
Enter the SPID Number (B channel 1 and B channel 2)	Enter the Service Profile Identifier (SPID) provided by your ISDN service provider for this B-channel.
B Channel Usage (B channel 1 and B channel 2)	<p>Select one of the following connection types:</p> <ul style="list-style-type: none"> ■ Local: This trunk is used for local PSTN calls only. ■ Remote: This trunk is used only for calls to and from the host PBX. ■ Local & Remote: This trunk can route both types of calls.

The following is a completed example.

Select the module that you want to configure.

Specify the switch and ISDN line type. (Get this information from your service provider.)

Enter the DN and SPID for each B-channel.

Specify whether each B-channel is to be used to process locally controlled calls, host-controlled calls, or both.

- 10 Repeat step 9 for each ISDN BRI module you want to configure.
- 11 Click on the **Next** button.

Result: The following screen displays:



12 Do one of the following:

IF you are performing an THEN

offline configuration,

1 Click on the **Save to File** button.

Result: Configuration Manager prompts you to specify the directory path and file name for the configuration file.

2 Specify the directory path and file name for this configuration.

Note: The file name automatically defaults with the name you entered as the node name.

3 Ensure the Files of type field shows Text File(*.TXT).

4 Click on the **Save** button to complete the Save to File.

Result: The file is saved, then you are asked if you want to configure another board. If you do, click on the **Yes** button, and continue with step 3 on page 120.

5 You can open the information in this file in Configuration Manager, then send and save the file in the RLC's Flash memory at another time. For instructions, refer to "Working with configuration files" on page 153.

IF you are performing an THEN

online configuration,

- 1 Click on the **Save to Flash** button.

Result: Configuration Manager writes the information entered to the Flash memory of the Remote Gateway 9150 unit you are configuring.

If successful, Configuration Manager displays the following message:

Data Sent Successfully

Note: Nortel recommends that you also save the configuration to a file.

- 2 Restart the Remote Gateway 9150 unit.
-

Testing the network connections

After you have installed the hardware and performed initial configuration, use the following methods to test the network connectivity:

- Test the Ethernet connection between the administration PC and the Remote Gateway 9150 unit. To perform this test, the following must be true:
 - You must be physically connected to the network.
 - You must be logged on to Configuration Manager.Refer to “Using Configuration Manager PING” on page 362 for complete details on performing a Configuration Manager PING.
- Check your telephone network connections.
- Perform a PSTN connectivity test. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for complete details.
- Perform a syslog test.
Refer to “Syslog testing” on page 365 for complete details on performing a syslog test.

Verifying telephone network connectivity

To verify the telephone network connectivity:

- 1 Look at the digital telephone display.
Does it display the correct time and date? If yes, then the connection paths between the digital telephone, Remote Gateway 9150 unit, and the RLC are working.
- 2 Lift the telephone handset, or press the host call appearance key to go off hook.
Did you receive a dial tone? If yes, then the connection path between the Remote Gateway 9150 unit and the RLC is working.
- 3 Initiate an outgoing call through the host PBX.
Did the call proceed as expected? If yes, then the connection path between the Remote Gateway 9150 unit and the RLC is working.

- 4 Press the local call appearance key to go off hook.
Did you receive a dial tone? If yes, then the connection path between the Remote Gateway 9150 unit and the digital telephone is working.
- 5 Initiate an outgoing call through the PSTN.
Did the call proceed as expected? If yes, then the ISDN BRI lines to the PSTN are working.

What to do if the telephone connection tests do not work

- 1 Ensure the Remote Gateway 9150 unit completed its power-up cycle successfully. If it did, the Status LED indicator remains lit.
- 2 Verify the connections between the telephone network and the Remote Gateway 9150 unit.
- 3 Ensure that the placement of ISDN BRI modules within the Remote Gateway 9150 unit correspond with the Telco 1 and Telco 2 cable connections.
Note: Refer to the Telco 1 and Telco 2 cable pin-out tables in Appendix C, "Pin-out tables for connections."
- 4 Use Configuration Manager to verify that the following configuration is correct on the Remote Gateway 9150 unit, as appropriate:
 - IP addresses (Remote Gateway 9150 unit, subnet mask, and default gateway, as well as the RLC's IP address, if the IP network is being used to route calls)
 - the telephone number used to establish connections to the RLC, if the PSTN is being used to route calls
 - the security IDs of both the Remote Gateway 9150 unit and the RLC, if a security ID is required to authenticate connection attempts
 - DNs and SPIDs assigned to the ISDN BRI modules installed in the Remote Gateway 9150 unit
 - station configuration, to ensure that the telephone you are using has the calling capabilities needed to complete the tests (that is, verify that the station is correctly configured as local only, remote only, or both local and remote)**Note:** For instructions on using Configuration Manager, refer to Chapter 5, "Configuring the Remote Gateway 9150 unit".

- 5 Work with the administrator at the host PBX site to ensure that
 - the RLC is enabled and working in its PBX slot (restart the RLC, if necessary)
 - the configuration of the IP address, telephone number, and security ID on the RLC port are correct (if these items are used)
- 6 Verify that both the telecom and data networks are routing voice calls as expected (that is, calls are not being blocked in any way).
- 7 Use Configuration Manager to examine the display logs for errors.

Note: Refer to the Configuration Manager Help application for a complete listing of all display logs and the condition indicated by each.

Chapter 4

Using Configuration Manager

In this chapter

What is Configuration Manager?	134
Starting and viewing Configuration Manager	135
Configuration Manager description	137
Using online Help	144
Configuration files description	145
Working with configuration files	153
Selecting the device type for offline configuration	156
Logging on to a unit	157
Logging off of the unit	166
Using the Remote Connection command	167
Performing a system restart or shutdown	169
Closing Configuration Manager	171
Uninstalling the Configuration Manager software	172

What is Configuration Manager?

Configuration Manager is a Windows-based software application that you install on your PC. Configuration Manager allows you to configure, administer, and upgrade the RLC. These tasks can be performed over either of the following connection types:

- 10BaseT Ethernet
- RS-232 serial

Note: It is not possible to use Configuration Manager to configure a Remote Gateway 9150 unit over a modem connection.

The CD shipped in the RLC package includes the Configuration Manager software. You can obtain the CD from your Nortel distributor or click on the **Software Downloads** link at the following website:

www.nortel.com

For the required characteristics of the Meridian administration PC, refer to “Windows PC requirements” on page 62.

To install the Configuration Manager software on your administration PC, refer to “Installing the Configuration Manager software” on page 113.

ATTENTION!

Complete all Remote Gateway 9150 unit configuration using Configuration Manager. Only use the man-machine interface (MMI) with the assistance of technical support personnel for troubleshooting and diagnostic testing.

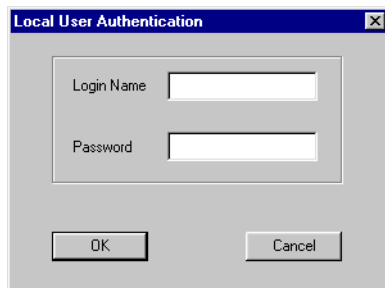
Starting and viewing Configuration Manager

The Configuration Manager software application is best viewed when your monitor settings are configured as 1024 by 768 pixels using Small Fonts at 96 dpi. If you use larger fonts, some fields and buttons might be hidden. You must use the horizontal and vertical scroll bars to view the hidden fields or buttons. For instructions on changing your display settings, refer to the Windows online help on your PC.

To start and log on to a Configuration Manager session:

- 1 From the Menu Bar, choose Start → Programs → Remote Gateway 9100 Series → Configuration Manager.

Result: The Configuration Manager opens prompts you for the logon name and password.



- 2 Enter **admin** in the Login Name field.
- 3 Enter **root** in the Password field.

Note: This is the default password. You can change the password after installation, though Nortel recommends that you do not change the password until your Remote Gateway 9100 Series system is up and running.

- 4 Click on the **OK** button.

Result: The system informs you of a successful logon. In the event of an unsuccessful logon, the system informs you of the need to re-enter the information.

- 5 Click on the **OK** button.

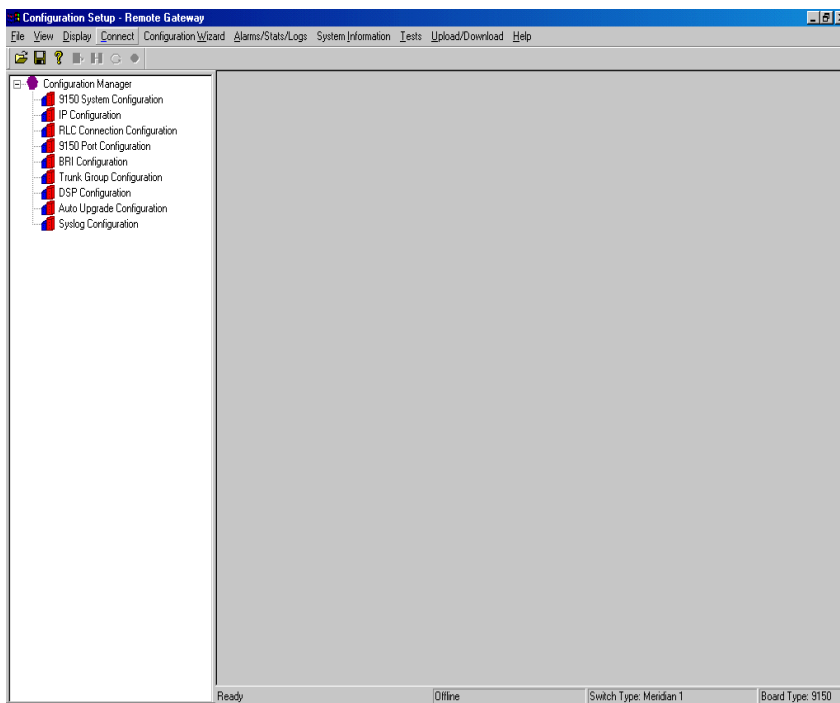
Result: The Local User Authentication dialog box closes.

- 6 Proceed as follows:

To perform an	refer to
online configuration,	“Logging on to a unit” on page 157.
offline configuration,	“Selecting the device type for offline configuration” on page 156.

- 7 To view the system tree, click on the plus sign (+) beside Configuration Manager in the left pane.

Result: Based on the system type you are working with, the system tree expands, showing you the types of configuration you can work with. An example is shown on page 136.



Note: When you first logon to Configuration Manager, the default system tree shows RLC configuration property sheets.

Configuration Manager description

This section describes each part of the Configuration Manager screens.

Parts of the Configuration Manager screen

The Configuration Manager is divided into three parts— a menu and two panes.

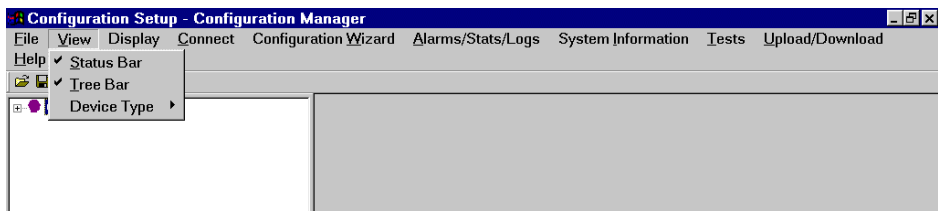
- The menu across the top of the screen lists various administrative tasks you can perform. These tasks are common to all Remote Gateway 9100 Series units.
- The pane on the left lists the property sheets you can work with. In this guide, the left pane is called the *system tree*.
- The pane on the right displays the screen associated with an item you selected from the system tree. In this guide, the right pane is called the *property sheet*.

Menu Bar

The Menu Bar across the top of the screen provides access to system display and reporting options.

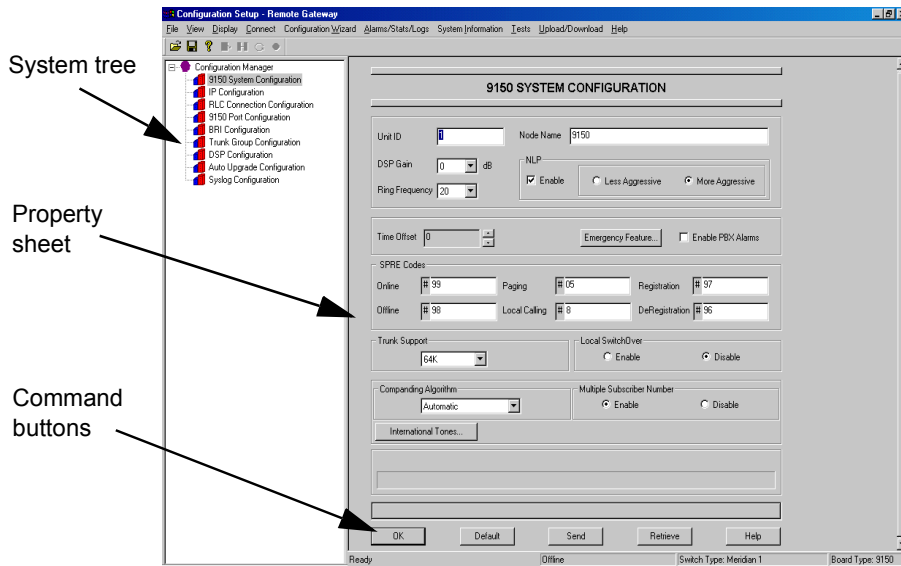
When you click on an option on the Menu Bar, a drop-down list displays. When you select an option from the drop-down list, the screen associated with that option displays.

Note: Dimmed options cannot be used for the unit you are working with, or if you are working offline (that is, when you are not logged on to any unit).



System tree

The left pane of the Configuration Manager lists property sheets you can work with. To view a list of all the property sheets associated with a system, click on the plus sign (+) to expand the list. (To hide the list, click on the minus sign [-].) With the System Tree expanded, click on a configuration to display the associated property sheet in the right pane, similar to the following:



To hide the system tree, choose View → Tree Bar from the Menu Bar. The screen redraws itself showing only the right pane and displaying the selected property sheet. To display the system tree again, choose View → Tree Bar.

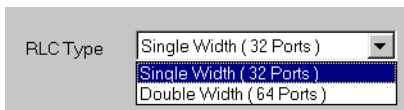
Property sheets

When you are logged on to a particular Remote Gateway 9100 Series unit (that is, a Remote Gateway 9150 unit or RLC), Configuration Manager displays a system tree specific to the logged-on unit.

When you click an item in the system tree, the associated property sheet displays in the right pane. For instructions on selecting a device type when not logged on, refer to “Selecting the device type for offline configuration” on page 156.

Drop down boxes

Boxes that provide a limited list of values are called *drop down boxes*. To view the values available for a drop down box, click on the down arrow for that box. To select an item from the list, move the cursor until the desired item is highlighted, and then click on the item. The item you select displays in the drop down box.



In some cases, selecting a particular list item causes the property sheet contents to change as follows:

- Dimmed (disabled) fields cannot be configured in the context of the list item you selected.
- Other fields are re-enabled (no longer dimmed).
- One or more values on the property sheet are replaced with values that are specific to the item you selected.

Check boxes

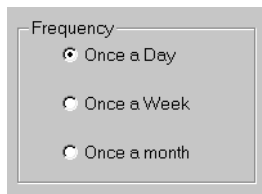
Fields that contain a blank box beside them are called *check boxes*. These check boxes are used to enable or disable the feature associated with that field. To enable the feature, click on the check box. A check mark displays. When you click on the check box again, the check box clears (thereby disabling the feature).



Option buttons

Some fields have multiple options. There is a circle beside each option that is called an *option button*. For these fields, you can only select one option.

To enable an option, click on its associated option button. If you change a previously selected option, the previously selected option button clears.



In some cases, selecting a particular option button causes the property sheet contents to change as follows:

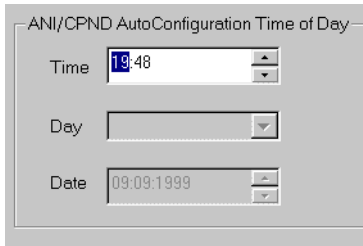
- When a field is dimmed (disabled), it cannot be configured in the context of the option you selected.
- Other fields are re-enabled (no longer dimmed).
- One or more values on the property sheet are replaced with values that are specific to the option you selected.

Scroll boxes

Boxes that contain data with up and down arrows beside them are called *scroll boxes*. When you click on the data, and then the up arrow, the selected data increases in value. When you click on the down arrow, the selected data decreases in value.

You can also change the data by manually entering it. To do so, highlight the data you want to change, and then type over it.

The following screen is an example of a scroll box:



ANI/CPND AutoConfiguration Time of Day

Time 18:48

Day

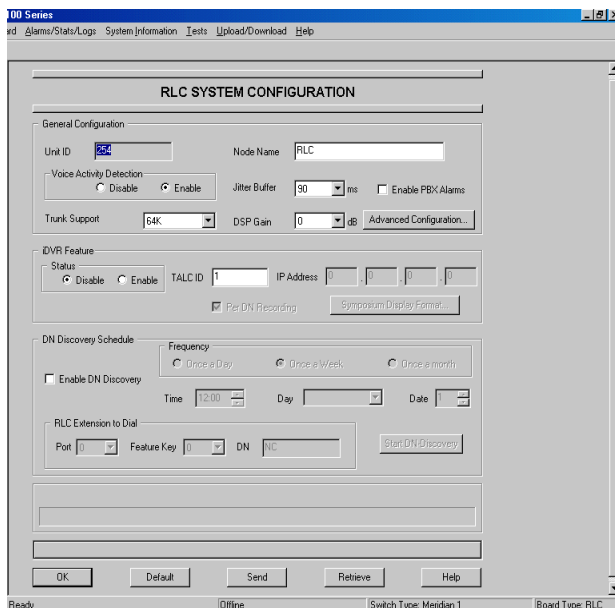
Date 09:09:1999

Scroll bars

If your monitor's display settings are configured so that not all the information can be displayed at once, horizontal and vertical scroll bars might display in Configuration Manager. Some fields and buttons might be hidden. An example is shown on the next page.

The Configuration Manager software application is best viewed when your monitor settings are configured as 1024 by 768 pixels using Small Fonts at 96 dpi. This ensures that all fields and buttons are visible.

For instructions on changing your display settings, refer to the Windows online Help on your PC.



You can prevent these scroll bars from displaying by changing the screen area pixel and font sizes in the Windows Control Panel display settings on your PC.

Command buttons

The following buttons display on every property sheet listed in the first level of the 9150 Configuration Manager system tree (left pane):

- **OK**
Click on this button to accept any changes you have made to the displayed property sheet. This command stores these values in a temporary file on your PC until you are ready to update the unit's Flash memory. For more details, refer to "OK" on page 148.
- **Default**
Click on this button to insert default values into every field in the displayed property sheet.
- **Send**
Click on this button to update the buffer of the unit you are logged on to with the values currently on the displayed property sheet. For more details, refer to "Send" on page 149.
- **Retrieve**
Click on this button to display the saved configuration value for every field on the displayed property sheet from the unit's local buffer. The unit's local buffer contains the last sent data. For more details, refer to "Retrieve" on page 150.
- **Help**
Click on this button to display online Help for the property sheet you are working with. For other methods of displaying Help, refer to "Using online Help" on page 144.

Using online Help

While using Configuration Manager, you might have questions about what certain boxes and buttons do, as well as how to complete certain tasks. Online Help provides brief answers to such questions.

To access Help:

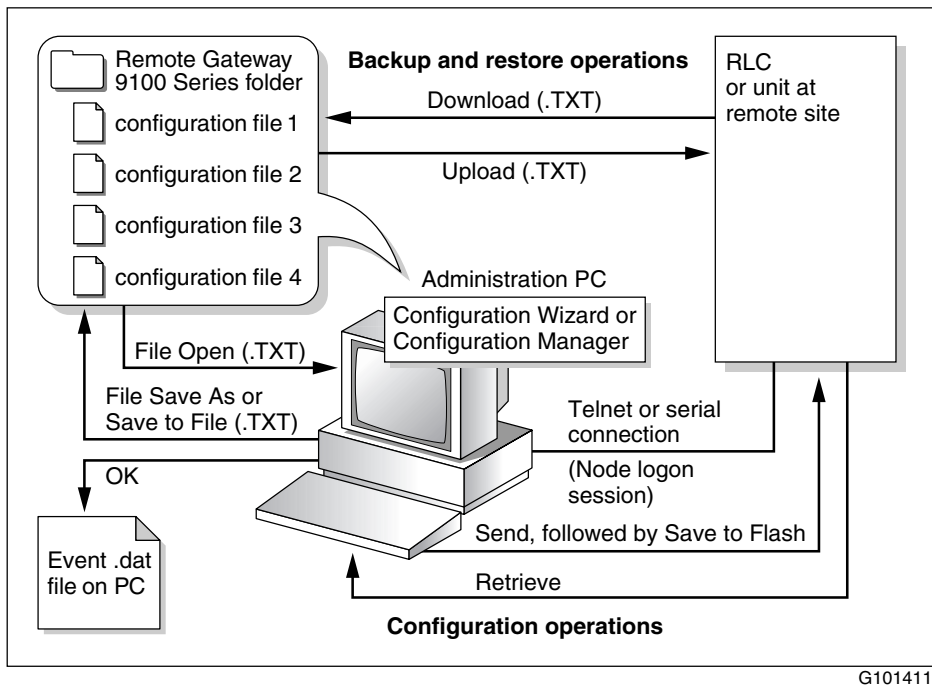
- 1 Use one of the following methods:
 - Method 1: Click on the **Help** button to get information concerning the active property sheet.
 - Method 2: From the Menu Bar, choose Help → Help Topics.
 - Method 3: Click on the **?** in the toolbar.
 - Method 4: Press **F1** on the keyboard.
- 2 If you selected methods 2, 3, or 4, go to one of the following tabs, based on how you want to search for a topic:
 - To refer to a list of Help topics, click on the **Contents** tab.
 - To look up a subject alphabetically, click on the **Index** tab.
 - To do a full-text search to find topics that contain the words you enter, click on the **Find** tab.

Configuration files description

This section describes configuration files and the ways that you can work with them.

Configuration Manager: File operations diagram

The following diagram shows how configuration information is stored. A detailed description of each file type and operation follows.



Types of files

You can work with three types of files in Configuration Manager. Each file is identified by one of the file name extensions described in the following table:

File name	File type	When it is created and used
event.dat	Log file	<p>The log (event.dat) file records all activities (and messages associated with those activities) that you perform while running Configuration Manager, such as:</p> <ul style="list-style-type: none">■ logging on to Configuration Manager■ logging on to a unit (by serial or Telnet connection)■ logging off of the unit■ performing configuration changes■ performing firmware upgrades <p>This file can be very useful when troubleshooting system problems. Technical support personnel may ask for this file.</p> <p>Note: Information is appended to this file each time you start a new Configuration Manager session.</p>
*.txt	Text	<p>The text (.txt) file is created when you do one of the following:</p> <ul style="list-style-type: none">■ Click on the Save to File button while running the Configuration Wizard.■ Choose File → Save As from the Menu Bar while working in Configuration Manager.■ Choose Upload/Download → Download Configuration from the Menu Bar to save a unit's configuration in a text file on the administration PC.

File name	File type	When it is created and used
*.txt (continued)	Text	<p>To view or make changes to the text file (while in online or offline mode), do one of the following to open the file:</p> <ul style="list-style-type: none"> ■ Click on the Open button while running the Configuration Wizard. ■ Choose File → Open from the Menu Bar while running Configuration Manager. ■ Choose Upload/Download → Upload Configuration from the Menu Bar to load the configuration file to the unit's buffer. <p>For more details about these tasks, refer to</p> <ul style="list-style-type: none"> ■ “Working with configuration files” on page 153 ■ “Creating a backup configuration file” on page 282 ■ “Restoring the configuration” on page 285 <p>Note: You can view or edit the contents of the text file by opening it in a word processing application, such as WordPad.</p>
*.upg	Upgrade	<p>Use the upgrade (.upg) file when performing firmware upgrades. For more details, refer to “Performing a firmware upgrade” on page 338.</p>

Configuration Manager: File operations description

The following table describes each operation shown in the “Configuration Manager: File operations diagram” on page 145.

Operation	Description
OK	<p>When you click on the OK button, the following occurs:</p> <ul style="list-style-type: none">■ Configuration Manager checks any changes you made for errors that, if found, produce an error dialog box. If Configuration Manager displays an error dialog box, make the necessary changes, and then click on the OK button again.■ The changes you make are stored in the event.dat file on your PC. For more information about the event.dat file, refer to “Types of files” on page 146. <p>Note: You must click on the OK button after making changes to a property sheet. However, your changes are not yet saved</p> <p>After clicking on the OK button, you can send the changes to the logged on unit’s buffer using a Send or Send All command. You can now update the Flash memory of the logged on unit by performing an Upload/Download → Save to Flash operation from the Menu Bar. For more details, refer to “Send” on page 149.</p> <p>Note: If you do not click on the OK button on a property sheet before displaying another property sheet, you lose all of the changes made on the first property sheet. To regain lost changes, you must reenter them.</p>
File → Open	<p>When you choose File → Open from the Menu Bar, you can open a previously saved configuration file. This is useful for preparing and storing configuration files in a central location before they are deployed to the network.</p> <p>Note: To open a file, the file type must be text (.txt).</p>

Operation	Description
File → Save As	<p>When you choose File → Save As from the Menu Bar, Configuration Manager saves the unit's configuration to a file on your PC. You must specify the file name and directory location.</p> <p>After saving the file, you can open and modify it at a later time.</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ Configuration Manager saves the file as a text (.txt) file. ■ If you close Configuration Manager without choosing File → Save As, you lose all of the changes you made.
Send	<p>When you click on the Send button, Configuration Manager sends any changes made on the displayed property sheet to the buffer of the logged-on unit. If the send is successful, the following message displays:</p> <p>Data Sent Successfully</p> <p>(Nortel recommends that you click on the OK button before clicking on the Send button.)</p> <p>Note: You must choose Upload/Download → Save to Flash from the Menu Bar to save the changes to the unit's Flash memory. For more details, refer to "Save to Flash" on page 150.</p>
Send All	<p>When you choose Upload/Download → Send All on any property sheet, changes for <i>all</i> property sheets pertaining to the logged-on unit are sent to the buffer on the unit you are connected to. If the send is successful, the following message displays:</p> <p>Data Sent Successfully</p> <p>Note: You must choose Upload/Download → Save to Flash from the Menu Bar to save the changes to the unit's Flash memory. For more details, refer to "Save to Flash" on page 150.</p>

Operation	Description
Retrieve	<p>When you click on the Retrieve button on a property sheet, the configuration stored in the buffer of the unit that you are connected to (the latest configuration information) displays in Configuration Manager.</p> <p>If the retrieval is successful, the following message displays:</p> <p>Data Received Successfully</p>
Save to Flash	<p>When you choose Upload/Download → Save to Flash from the Menu Bar, the information stored in the logged-on unit's buffer is saved to Flash memory. This prevents the configuration from being lost if the unit loses power.</p> <p>While in progress, the following message displays in the status bar at the bottom of the screen:</p> <p>Save to Flash</p> <p>When the Save to Flash is completed, the Data Stored to Flash dialog box displays.</p> <p>Some changes require a restart of the unit after saving the changes. If a restart is necessary, Configuration Manager prompts you to do so.</p> <p>Notes:</p> <ul style="list-style-type: none">■ You must click on the Send button or choose Upload/Download → Send All from the Menu Bar <i>before</i> you choose Upload/Download → Save to Flash. Perform a Save to Flash as often as you think it is necessary, to keep your configuration information safe. <p>Note: Do not ignore error messages in the Save to Flash process. If Save to Flash fails, retry uploading and saving to Flash. If the problem persists, check the file being uploaded and report the problem to Nortel.</p>

Operation	Description
Upload Configuration	<p>When you choose Upload/Download → Upload Configuration from the Configuration Manager menu, the configuration file you specify is uploaded and written to the buffer on the active unit.</p> <p>Use this option if you need to restore or replace an entire configuration.</p> <p>You must perform a Save to Flash from the Upload/Download Menu to save the changes in the unit's Flash memory. If you do not perform a Save to Flash and a power loss occurs on the unit, the changes are lost.</p> <p>While in progress, Save to Flash in Progress displays in the status bar at the bottom of the screen.</p> <p>When the Save to Flash is completed, the Data Stored to Flash dialog box displays.</p> <p>Notes:</p> <ul style="list-style-type: none">■ To upload a configuration file, the file type must be text (.txt).■ To perform a configuration upload over the IP network, a TFTP server application must be running on your PC. Uploads over the serial port are not supported.■ The upload operation does not affect the event.dat file on the PC.■ The new configuration does not take effect until you restart the unit. For instructions on how to restart the unit, refer to “Performing a system restart or shutdown” on page 169.■ If the upload fails or aborts, confirm that you are uploading the correct file. If the problem persists, contact Nortel technical support for assistance.

Operation	Description
Download Configuration	<p>When you choose Upload/Download → Download Configuration from the Menu Bar, Configuration Manager saves the configuration stored on the logged-on unit to a file on the PC.</p> <p>Use this option if you want to create a backup of the unit's configuration.</p> <p>Notes:</p> <ul style="list-style-type: none">■ The downloaded file is saved as a text file (.txt).■ The download operation does not affect the event.dat file on the PC. If you make changes and do not save them, you lose those changes.

Working with configuration files

This section explains how to:

- create a configuration file (refer to page 154)
- open a configuration file in Configuration Manager (refer to page 154)
- perform a configuration upload (refer to page 155)
- perform a configuration download (refer to page 155)

When to use the Configuration Manager file operations

You can use	When you are
OK, File → Open, and File → Save As	working in offline mode or connected and logged on to a unit. Note: When working in offline mode, you must save the configuration to a file. However, when you are logged on to a unit, the file save operation is optional. To save the configuration to Flash, first update the unit's local buffer by clicking on the Send button or choosing Upload/Download → Send All from the Menu Bar. Then, use Upload/Download → Save to Flash to complete the operation.
one of the following: <ul style="list-style-type: none">■ Send■ Send All■ Retrieve■ Upload Configuration■ Download Configuration	connected and logged on to a unit.

Creating a configuration file on the PC

To create a configuration file on the PC:

- 1 Start Configuration Manager.
- 2 Make the required changes on each property sheet.

Note: You do not have to be logged on to a unit to make configuration changes. When you are not logged on to a unit, you can perform an *offline configuration*.

- 3 From the Menu Bar, choose File → Save As.

Result: The Save As dialog box displays.

- 4 Enter a descriptive name for the file.

Use the file name to identify the type of configuration it contains.

Example 1: If the file contains a basic configuration that is to be used for a specific type of unit, enter **template** as the file name.

Example 2: If the file contains a configuration that is unique to a specific unit, enter the unit's name or number as the file name.

- 5 Ensure the Save as type drop down box shows Text Files(*.txt).
- 6 Specify the folder where you want to save the file.
- 7 Click on the **OK** button.

Result: The file is saved.

Note: Nortel strongly recommends that you do not manually edit this file.

Opening a configuration file

To open a configuration file:

- 1 Start Configuration Manager.
- 2 If you want to work in online mode, log on to the unit. Otherwise, ensure that you have selected the device type.
- 3 From the Menu Bar, choose File → Open.

Result: The Open dialog box displays.

- 4 Ensure the Files of type drop down box shows Text Files(*.txt).
- 5 Navigate to the folder containing the file you need.

- 6 Select the file, and then click on the **Open** button.

Result: The contents of the configuration file are loaded into Configuration Manager.

- 7 View the configuration details by clicking on each item in the system tree to display the associated property sheet.
- 8 Make changes as necessary, complete the following actions:
 - a. Save the file by choosing File → Save from the Menu Bar. If you want to change the file name, choose File → Save As from the Menu Bar.
 - b. Click on the **Send** button to update the unit, then choose Upload/Download → Save to Flash from the Menu Bar.

Uploading a configuration to a unit

For complete instructions on uploading a configuration to a unit, refer to “Restoring the configuration” on page 285.

Downloading a configuration from a unit

For complete instructions on downloading a configuration to a unit, refer to “Creating a backup configuration file” on page 282.

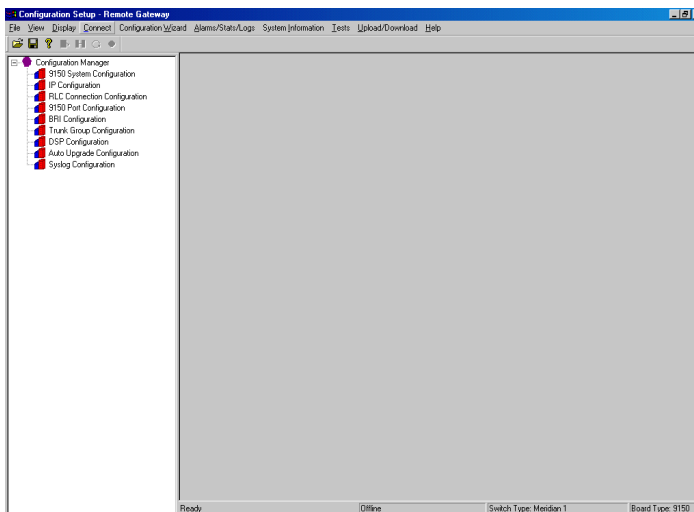
Selecting the device type for offline configuration

If you are not logged on to a Remote Gateway 9100 Series unit (that is, an RLC or a Remote Gateway 9150 unit), then you must select the device type you want to work with. Configuration Manager reorganizes the system tree with the property sheets associated with that device type.

To select the device type for offline configuration:

- 1 Start Configuration Manager as described in “What is Configuration Manager?” on page 134.
- 2 From the Menu Bar, choose View → Device Type, and the type of device (for example, RLC or 9150).
- 3 Click on the plus sign (+) beside Configuration Manager in the left pane.

Result: The system tree expands in the right pane, similar to the following:



Logging on to a unit

If you want to update the Flash memory on a unit as you make configuration changes, or view statistics and logs, you must log on to the unit. Each unit has its own administration ID and password.

You can log on to the unit by using one of the following connection methods:

- Telnet (over the IP network)
- serial port

Connection types

If the RLC or Remote Gateway 9150 unit is connected to the administration PC by the RS-232 cable, you can establish a connection through the serial port.

If Ethernet connectivity has been established between the administration PC and the RLC or Remote Gateway 9150 unit, you can establish an IP connection with Telnet.

Default logon ID and password

The default logon ID is **guest**. You cannot change the logon ID.

The default password is **guest123**. The password can be changed and, therefore, can be different if this is not a first time installation. Nortel recommends that you do not change the password until your 9150 system is up and running smoothly.

Connection history

Configuration Manager maintains a record of past unit connections. You can select, and then connect to a unit from the history list that displays in the Connect menu.

Note: Upgrading the Configuration Manager software deletes the connection history list.

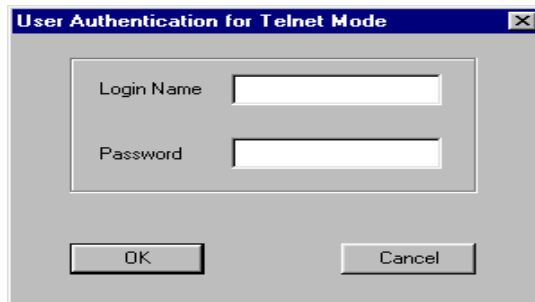
Auto logoff

If the connection remains open with no activity for 15 minutes, then Configuration Manager automatically logs off the connection and the Session Timed Out message displays. This helps to secure the configuration in the event that you walk away from the administration PC while logged on to a unit.

Logging on to a unit using the connection history

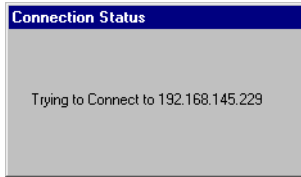
- 1 From the Menu Bar, choose Connect → XXX.XXX.XXX.XXX (IP address of the unit you want to log on to).

Result: If no one else logged on to the unit before you and if IP connectivity exists to this unit, the User Authentication for Telnet Mode dialog box displays. It is similar to the following:



- 2 Enter your logon name in the Login Name field. If you have not yet customized this setting, refer to "Default logon ID and password" on page 157 for the default logon ID.
- 3 Enter your password in the Password field. If you have not yet customized this setting, refer to "Default logon ID and password" on page 157 for the default password.
- 4 Click on the **OK** button.

- 5 Configuration Manager initiates a connection attempt. The Connection Status message box displays. It is similar to the following:



Note: The connection speed can be too fast for this message to be seen in a successful logon attempt.

If you do not enter any logon information, after two minutes Configuration Manager displays a reminder dialog box similar to the following:

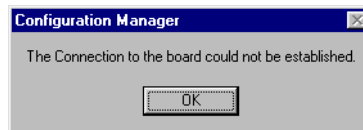


Click on the **OK** button to return to Step 2 on page 158.

IF the logon attempt THEN

fails,

a message box similar to the following displays:



Complete the following actions:

- 1 Click on the **OK** button.
- 2 Go back to Step 1 on page 158 to try again.

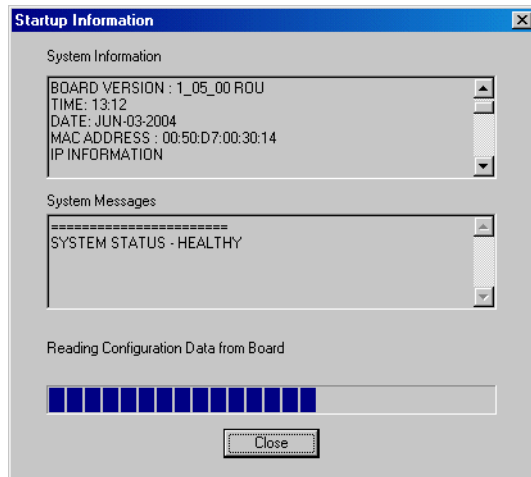
IF the logon attempt THEN

is successful,

the User Logged In dialog box displays.

Click on the **OK** button.

Result: The Startup Information dialog box displays. It is similar to the following:



Messages display above the progress bar at the bottom of the dialog box, similar to the following:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from Flash memory.

When initialization is complete, the Configuration Data Read Successfully message displays above the progress bar.

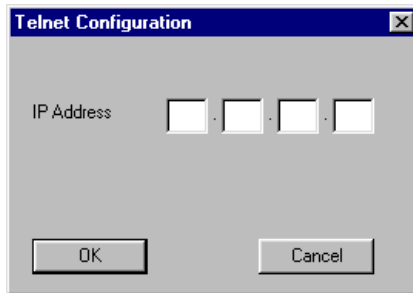
Click on the **Close** button.

Logging on to a unit using Telnet

To log on to a unit using Telnet:

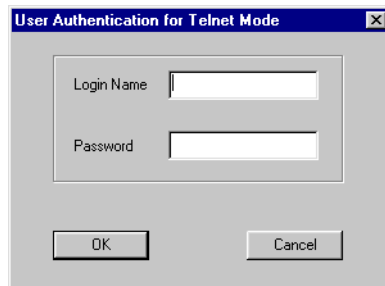
- 1 From the Menu Bar, choose Connect → Logon Unit → Telnet.

Result: The Telnet Configuration dialog box displays, similar to the following:



- 2 Enter the IP Address of the unit you want to connect to.
- 3 Click on the **OK** button.

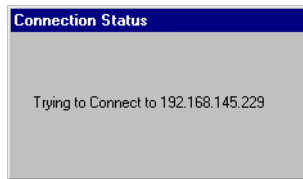
Result: If no one else logged on to the unit before you, and if IP connectivity exists to this unit, the User Authentication for Telnet Mode dialog box displays, similar to the following:



- 4 Enter your logon name in the Login Name field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 157 for the default logon ID.
- 5 Enter your password in the Password field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 157 for the default password.

6 Click on the **OK** button.

Result: Configuration Manager initiates a connection attempt. The Connection Status message box displays. It is similar to the following:



Note: The connection speed can be too fast for this message to be seen in a successful logon attempt.

If you do not enter any logon information, after two minutes Configuration Manager displays a reminder dialog box similar to the following:

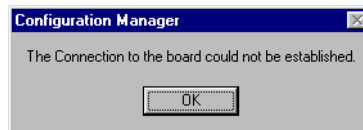


Click on the **OK** button to return to Step 4 on page 161.

IF the logon attempt THEN

fails,

a message box similar to the following displays:



Complete the following actions:

- 1 Click on the **OK** button.
- 2 Go back to Step 1 on page 161 to try again.

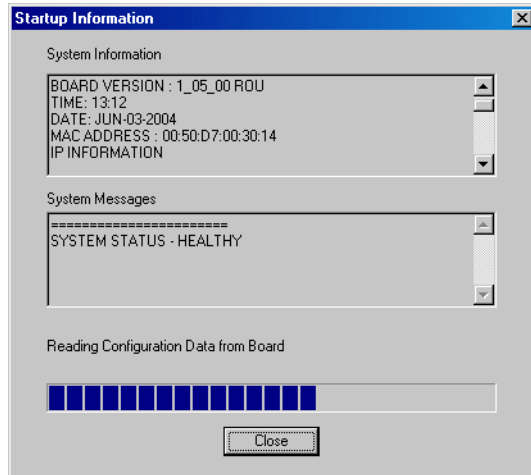
IF the logon attempt THEN

is successful,

the User Logged In dialog box displays.

Click on the **OK** button.

Result: The Startup Information dialog box displays. It is similar to the following:



Messages display above the progress bar at the bottom of the dialog box, similar to the following:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from Flash memory.

When initialization is complete, the Configuration Data Read Successfully message displays above the progress bar.

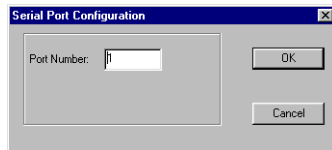
Click on the **Close** button.

Logging on to a unit using the serial port

To log on to a unit using the serial port:

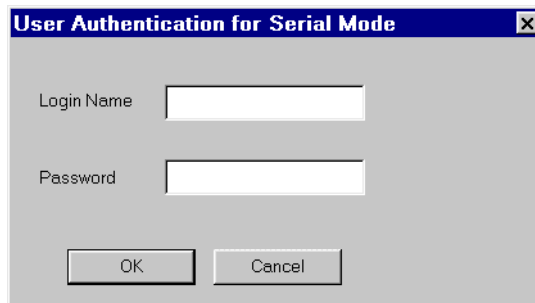
- 1 From the Menu Bar, choose Connect → Logon Unit → Serial.

Result: The Serial Port Configuration dialog box displays, similar to the following:



- 2 Enter the COM port number the unit is connected to in the Port Number field.
- 3 Click on the **OK** button.

Result: If no one else logged on to the unit before and if your PC is connected with a serial cable to the Remote Gateway 9150 unit, the User Authentication for Serial Mode dialog box displays. It is similar to the following:



- 4 Enter your logon name in the Login Name field. Refer to “Default logon ID and password” on page 157 for the default logon ID if you have not yet customized this setting.
- 5 Enter your password in the Password field. Refer to “Default logon ID and password” on page 157 for the default password if you have not yet customized this setting.

6 Click on the **OK** button.

Result: The connection attempt is initiated. The following message might display:

Trying to Connect via Serial Port <port number>

IF the logon attempt THEN

fails,

the following message displays:

SERIAL CONNECTION FAILED

Check the serial port connection and ensure it is good. Then, go back to step 1.

is successful,

the User Logged In dialog box displays.

Click on the **OK** button.

Result: The Startup Information dialog box displays.

Messages display above the progress bar at the bottom of the dialog box, similar to the following:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from Flash memory.

When initialization is complete, the Configuration Data Read Successfully message displays above the progress bar.

Click on the **Close** button.

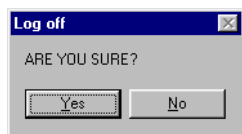
Logging off of the unit

When you are finished using Configuration Manager to make configuration changes, or to view logs and statistics, log off of the unit. Logging off secures the unit's configuration.

To log off of a unit:

- 1 From the Menu Bar, choose Connect → Logoff Unit.

Result: The Log off dialog box displays, similar to the following:



- 2 Click on the **Yes** button.

Result: The Configuration Manager: User Logged off dialog box displays, similar to the following:



- 3 Click on the **OK** button.

Using the Remote Connection command

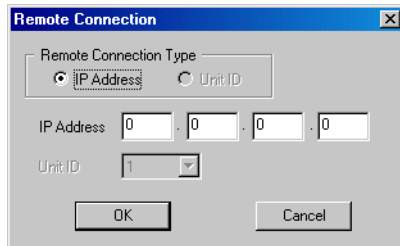
Use the Remote Connection command to log on to multiple Remote Gateway 9100 Series units during a single Configuration Manager session.

Note: Configuration Manager does not allow multiple users to log on to the same Remote Gateway 9100 Series unit simultaneously. To allow subsequent users to log on at a later time, you must log off of all Remote Gateway 9100 Series units that you have accessed before ending your Configuration Manager session.

The Remote Connection command allows you to move between Remote Gateway 9100 Series units without logging off from the current unit before logging on to another unit. After you log on to one unit using the Connect → Logon Unit command, log on to another unit using the following procedure:

- 1 From the menu, choose Connect → Remote Connection.

Result: The Remote Connection dialog box displays, similar to the following:



- 2 Do one of the following:
 - Click on the **IP Address** option button if you want to connect to the unit through the IP address.

Note: This option is available when you are logged on to any Remote Gateway 9100 Series unit.

- Click on the **Unit ID** option button if you want to connect to the unit through the Unit ID.

Note: This option is only available when you are logged on to an RLC. Use this option when accessing a Remote Gateway 9100 Series unit located behind a NAT router or Firewall device.

3 Do one of the following:

- Enter the IP address of the unit that you want to connect to in the IP Address fields.

Note: This option is available when you are logged on to any Remote Gateway 9100 Series unit.

- Enter the unit ID of the unit that you want to connect to in the Unit ID field.

Note: This option is only available when you are logged on to an RLC. Use this option when accessing a Remote Gateway 9100 Series unit located behind a NAT router or Firewall device.

4 Click on the **OK** button.

Result: Configuration Manager initiates a connection attempt. The following message can appear:

Trying to Connect to <IP address> or <unit ID>

Refer to “Logging on to a unit” on page 157 for more information.

When you complete your work on a unit, you must log off from that unit. Execute a Connect → Logoff Unit command for each unit that you logged on to before ending your Configuration Manager session.

Performing a system restart or shutdown

Configuration Manager allows you to perform a controlled system restart or shutdown.

When to perform a restart or shutdown

Each time that you make a configuration change, perform a Save to Flash. You must also restart the unit if Configuration Manager prompts you to do so.

Note: When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds. Some configuration changes do not take effect until the unit has been re-started.

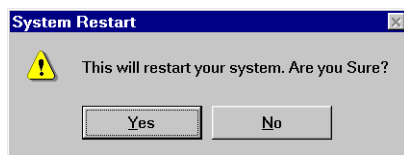
You can perform a system shutdown when you need to power the system down.

Performing a system restart

To perform a system restart:

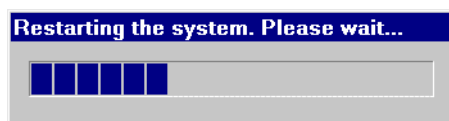
- 1 From the Menu Bar, choose Connect → System Reset → Restart.

Result: The System Restart dialog box displays, similar to the following:



- 2 Click on the **Yes** button.

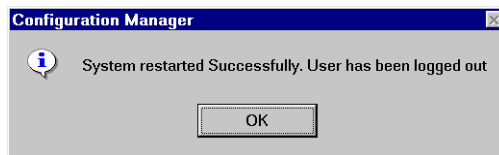
Result: The following status dialog box displays:



The following message also displays in the status bar at the bottom of the screen:

Restarting the System

The status continues to show Online. When the system restart is complete, a dialog box displays informing you that the system restart was successful, and that you are logged off, similar to the following:



- 3 Click on the **OK** button.

Result: Configuration Manager prompts you to log back on using the previous connection method (Serial or Telnet).

Performing a system shutdown

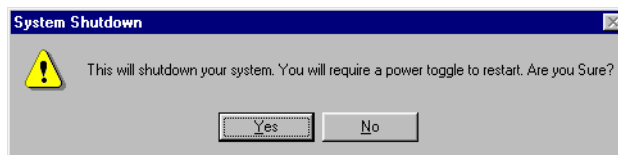
ATTENTION

Do not perform this procedure if you do not have physical access to the unit. To recover from the system shutdown, you must power the unit off, and then power it back on.

To perform a system shutdown:

- 1 From the Menu Bar, choose Connect → System Reset → Shutdown.

Result: The System Shutdown dialog box displays, similar to the following:



- 2 Click on the **Yes** button.

Result: Configuration Manager disconnects your logon session and the following message displays in the status bar at the bottom of the screen:

Shutting Down the System

The status shows Offline.

- 3 Turn the power on the Remote Gateway 9100 Series unit off.

Note: You must turn the power off before you can power the unit back up.

Closing Configuration Manager

When you have completed all the configuration modifications you want to make, or are done viewing unit logs and statistics, log off and close the Configuration Manager application. This secures the configuration, preventing others from accessing it if you walk away from the administration PC while logged on to a unit.



CAUTION

Risk of configuration loss

If you close Configuration Manager without saving the changes you made to a file on your PC, or without updating the Flash memory of the unit you were working on, all changes are lost. You must reenter any changes you made.

To close Configuration Manager:

- 1 Ensure that you have saved all configuration changes by doing one or more of the following:
 - From the Menu Bar, choose File → Save As, then specify the name for the configuration file. The file is saved on the administration PC hard disk.
 - Update the Flash memory of the unit you are connected to by doing one of the following:
 - Click on the **Send** button on any property sheet, then choose Upload/Download → Save to Flash from the Menu Bar.
 - Click on the **Send All** button on any property sheet, then choose Upload/Download → Save to Flash from the Menu Bar.
 - If you have saved the changes to a file, choose Upload/Download → Upload Configuration from the Menu Bar. For instructions, refer to “Restoring the configuration” on page 285.
- 2 Log off by choosing Connect → Logoff Unit from the Menu Bar.
- 3 Choose File → Exit from the Menu Bar.

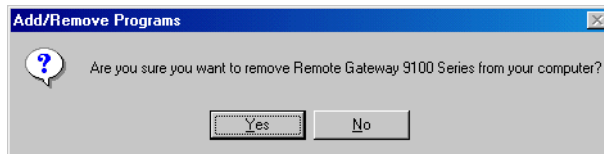
Result: Configuration Manager closes.

Uninstalling the Configuration Manager software

To remove the Configuration Manager software from your administration PC:

- 1 Choose Start → Settings → Control Panel.
- 2 Double-click on the **Add/Remove Programs** icon.
- 3 Select Remote Gateway 9100 Series from the list, and then click on the **Remove** button.

Result: The Add/Remove Programs dialog box displays, similar to the following:



- 4 Click on the **Yes** button.

Result: The Remote Gateway 9100 Series Configuration Manager is removed from the PC.

Chapter 5

Configuring the Remote Gateway 9150 unit

In this chapter

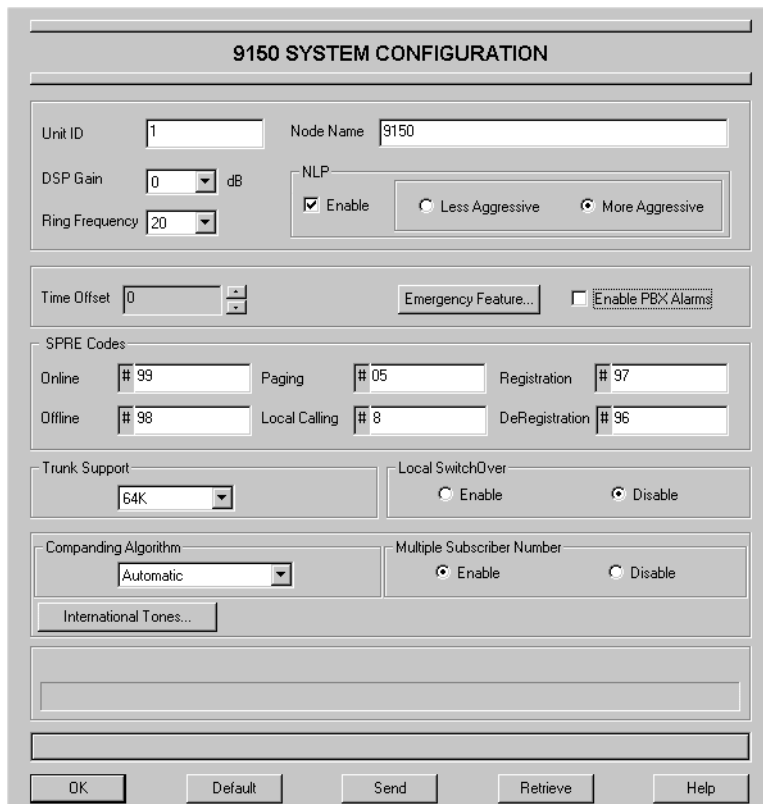
9150 System configuration	174
International tones support	186
IP configuration	192
RLC connection configuration	198
9150 port configuration	207
BRI configuration	225
Trunk group configuration	232
DSP configuration	239
Auto upgrade configuration	243
Syslog configuration	247
Station configuration	250

9150 System configuration

This section describes the settings that apply to the system rather than to the RLC port or Remote Gateway 9150 trunks or stations.

Getting there 9150 → Configuration Manager → 9150 System Configuration

9150 System Configuration property sheet



The image shows a software dialog box titled "9150 SYSTEM CONFIGURATION". It contains various settings for a 9150 unit. The settings are organized into several sections: Unit ID (1), Node Name (9150), DSP Gain (0 dB), Ring Frequency (20), NLP (Enabled, with radio buttons for Less Aggressive and More Aggressive), Time Offset (0), Emergency Feature... (with a checkbox for Enable PBX Alarms), SPRE Codes (Online: #99, Paging: #05, Registration: #97, Offline: #98, Local Calling: #8, DeRegistration: #96), Trunk Support (64K), Local SwitchOver (Disable), Companding Algorithm (Automatic), Multiple Subscriber Number (Enable), and International Tones... (button). At the bottom are buttons for OK, Default, Send, Retrieve, and Help.

9150 SYSTEM CONFIGURATION	
Unit ID	1
Node Name	9150
DSP Gain	0 dB
Ring Frequency	20
NLP	<input checked="" type="checkbox"/> Enable <input type="radio"/> Less Aggressive <input checked="" type="radio"/> More Aggressive
Time Offset	0
Emergency Feature...	<input type="checkbox"/> Enable PBX Alarms
SPRE Codes	
Online	# 99
Paging	# 05
Registration	# 97
Offline	# 98
Local Calling	# 8
DeRegistration	# 96
Trunk Support	64K
Local SwitchOver	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Companding Algorithm	Automatic
Multiple Subscriber Number	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
International Tones...	
OK	Default
Send	Retrieve
Help	

NLP

The Non-Linear Processor (NLP) works with the Remote Gateway 9100 Series echo canceller to reduce echo. Echo occurs in a telephone call when the transmitted signal reflects and is received by the transmitting device. To cancel the echo, the Remote Gateway 9100 Series system monitors the audio stream looking for echo. When echo is identified it is digitally (mathematically) removed. If the echo is very strong, a small amount of echo may remain called “residual” echo. The aggressiveness of the NLP determines how quickly and how effectively the Remote Gateway 9100 Series NLP reduces the residual echo.

The operation of the NLP can affect how the audio sounds during double-talk situations - when both parties are speaking. Cultural differences also change how often double-talk occurs during a conversation.

Nortel recommends the following settings as a starting point:

- RLC: NLP Enabled - Less Aggressive (default)
- 9150: NLP Enabled - More Aggressive (default)

If the Remote Gateway 9150 unit user hears echo during conversations, adjust the settings, as follows:

- RLC: NLP Enabled - More Aggressive
- 9150: NLP Enabled - Less Aggressive

If the party on the PBX side hears echo during conversations, adjust the settings, as follows:

- RLC: NLP Enabled - More Aggressive
- 9150: NLP Enabled - More Aggressive

The NLP does not have to operate aggressively if echo is not present. If echo is not present but double-talk is present, even with Less Aggressive settings, try disabling the NLP on the RLC.

Upgrades

When you perform a Remote Gateway 9150 firmware upgrade from release 1.3.4 or earlier, NLP settings return to their default values.

Emergency service programmability

The Remote Gateway 9150 unit can serve the emergency needs of telephones in multiple locations having different dialing plans. To access the Emergency Activation Code dialog box, click on the **Emergency Feature** button. You can configure up to three separate numbers to reach local emergency services regardless of which call appearance key you use to dial the number. The particular emergency activation code dialed by the user determines the digits sent to the host PBX and the telephone number sent to the Central Office (CO).

Also, in their haste to reach an emergency service, some users can forget to dial trunk access digits. You can configure your Remote Gateway 9150 unit to send the emergency telephone number to the CO whether or not the user dials trunk access digits.

Note: If you must contact emergency personnel with consecutive calls, you must press the digits of the Emergency Access Code each time. Do not use last number re-dial or the auto-dial keys.

Refer to the “Emergency Feature” on page 180 for further configuration details.

Configuring the Remote Gateway 9150 system settings

To configure the Remote Gateway 9150 system settings:

- 1 Complete the fields as described in “9150 System Configuration field descriptions” on page 178.
- 2 Click on the **OK** button to save the information in the temporary work file.

- 3 To update the Remote Gateway 9150 unit with the new information, click on the **Send** button.

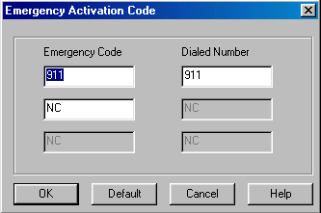
IF you are	THEN
logged on to the Remote Gateway 9150 unit,	the changes are written into the Remote Gateway 9150 unit's buffer. To save the changes in Flash memory, choose Upload/Download → Save to Flash from the Menu Bar.
not logged on to the Remote Gateway 9150 unit,	the Connection not Established dialog box displays: Do one of the following: <ul style="list-style-type: none">■ Log on to the Remote Gateway 9150 unit, and then click on the Send button again.■ Save the changes to a file on your administration PC.

Note: When you change System configuration parameters and Save to Flash, calls can be dropped. Ensure that there are no active calls when you make changes to these parameters.

9150 System Configuration field descriptions

Field	Description
Unit ID	<p>Enter a unique number from 1 through 20 to identify this Remote Gateway 9150 unit and differentiate it between the RLC and all remote units connected to the same RLC.</p> <p>Note: This is the same number that you enter in the Unit ID field of the RLC's Remote Connection Configuration property sheet for this Remote Gateway 9150 unit.</p> <p>The default is 1.</p>
Node Name	<p>Enter your site name.</p> <p>The node name uniquely identifies this Remote Gateway 9150 site in the RLC network.</p> <p>The default is 9150.</p>
DSP Gain	<p>Configure the DSP Gain if the voice levels at the distant site are too loud or quiet and cannot be resolved using the volume control on the telephone set. Positive values for the gain boosts the voice level for all remote calls to the distant site. Negative values for the gain reduce the voice level at the distant site for all remote calls.</p> <p>Select the number of decibels (dB) that you want to add to, or subtract from, the strength of the transmitted signal before the DSP processes it.</p> <p>Valid options are 9, 6, 3, 0, -3, -6, -9, -12, and -15.</p> <p>The default is 0 dB.</p>

Field	Description
NLP	<ul style="list-style-type: none">■ Click in the Enable checkbox to enable non-linear processing, or echo cancellation. <p>The default is selected.</p> <ul style="list-style-type: none">■ Click on the Less Aggressive option button if you choose to enable the NLP and echo is a significant problem on calls supported by your Remote Gateway 9100 Series unit.■ Click on the More Aggressive option button if you choose to enable the NLP but echo is not a significant problem on calls supported by your Remote Gateway 9100 Series unit. <p>The default is Less Aggressive.</p> <p>Refer to “NLP” on page 175 for information on the proper configuration of NLP settings.</p>
Ring Frequency	<p>Certain devices-most notably, some European fax machines-only recognize a ring frequency of 25 Hertz (Hz). Some telephones use a 20 Hz ring frequency. Remote Gateway 9150 units connected to fax machines that only recognize a 25 Hz ring frequency can require a different Ring Frequency setting. To change this setting, select 25 from this drop down list box.</p> <p>Valid options are 20 and 25.</p> <p>The default is 20.</p>
Time Offset	<p>Click on the up or down arrow to change the time zone difference between this Remote Gateway 9150 unit and the RLC.</p> <p>Note: Time Offset is in 15-minute intervals to a maximum of, plus or minus, 24 hours.</p> <p>The default is 0.</p>

Field	Description
Emergency Feature	<p>Click on the Emergency Feature button to configure emergency activation codes.</p> <p>Result: The Emergency Activation Code dialog box displays.</p>  <ul style="list-style-type: none"> ■ Emergency Code <p>Enter the number that the user must dial to tell the PBX to send to the CO the emergency service telephone number in the Dialed Number field immediately to the right.</p> <p>The first default is 911. Subsequent defaults are NC (Not Configured).</p> ■ Dialed Number <p>Enter the DN of the emergency service that you want the PBX to send to the CO when the user dials the Emergency Code in the field immediately to the left.</p> <p>The first default is 911. Subsequent defaults are NC (Not Configured).</p> <p>Note: Enter only the Emergency Activation Code (for example, 911 in North America). Do not include the trunk access code because the Emergency Activation code dials out directly on the PSTN.</p> <p>If you are using only the IP network to route calls, leave this field blank.</p> <p>Click on the OK button.</p> <p>Refer to “Emergency service programmability” on page 176 for further details on this feature.</p>

Field	Description
Enable PBX Alarms	<p>Click on the Enable PBX Alarms checkbox if you want the Remote Gateway 9150 unit to notify the host PBX to produce alarms and alerts. If you don't want the Remote Gateway 9150 unit to notify the host PBX to produce alarms and alerts, ensure that the Enable PBX Alarms checkbox is not selected.</p> <p>Refer to “Display logs” on page 412 to determine which alarms and alerts the PBX generates.</p>
SPRE Codes: Online	<p>Enter the SPRE code that is to be used to put your site into online mode, or accept the default code. The default code is #99.</p> <p>Note: The SPRE code is automatically prefixed with the pound sign (#). This means users must dial # before the SPRE code when going into online mode.</p> <p>Maximum length: 3 digits in addition to the pound sign</p> <p>Refer to “Online/offline table” on page 40 for more information.</p>
SPRE Codes: Paging	<p>Enter the SPRE code that is used to announce pages to other stations in your office, or accept the default code. The default is #05.</p> <p>Note: The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when initiating a page.</p> <p>Maximum length: 3 digits in addition to the pound sign</p>

Field	Description
SPRE Codes: Registration	<p>Enter the SPRE code that allows a multi-user or port-sharing participant to begin a session, or accept the default code. The default is #97.</p> <p>Note: The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when registering for a port.</p> <p>Maximum length: 3 digits in addition to the pound sign</p>
SPRE Codes: Offline	<p>Enter the SPRE code that is used to put your site into offline mode, or accept the default code. The default is #98.</p> <p>Note: The SPRE code is automatically prefixed with the pound sign (#). This means users must dial # before the SPRE code when going into offline mode.</p> <p>Maximum length: 3 digits in addition to the pound sign</p>
SPRE Codes: Local Calling	<p>Enter the SPRE code that allows analog or ATA-equipped station users to change the outgoing call mode to locally controlled mode. The default is #8.</p> <p>Note: The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when initiating a local call on an analog or ATA-equipped station.</p> <p>Maximum length: 3 digits in addition to the pound sign</p>
SPRE Codes: DeRegistration	<p>Enter the SPRE code that will allow a multi-user or port sharing participant to end a session, or accept the default code. The default is #96.</p> <p>Note: The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when disengaging from a port.</p> <p>Maximum length: 3 digits in addition to the pound sign</p>

Field	Description
Trunk support	<p data-bbox="461 240 1139 337">Choose 56K if you know that your Remote Gateway 9150 unit is in a PSTN network that can only transport at 56 Kbps.</p> <p data-bbox="461 354 1139 451">Choose 64K if you know that your Remote Gateway 9150 unit is in a PSTN network that can only transport at 64 Kbps.</p> <p data-bbox="461 467 1139 638">Choose Dynamic if you know that your Remote Gateway 9150 unit is in a PSTN network that supports speeds that vary from 64 Kbps to 56 Kbps. The Remote Gateway 9100 Series system dynamically adapts and downgrades a call to 56 Kbps if 64 Kbps is not available.</p> <p data-bbox="461 654 1127 751">Note: You must configure the same BRI speed (such as 56K, 64K, or dynamic) on both the RLC and the Remote Gateway 9150 unit.</p> <p data-bbox="461 776 683 803">The default is 64K.</p>

Field	Description
Local SwitchOver	<ul style="list-style-type: none">■ Click on the Enable option button to automatically route the voice path for local station-to-station calls (calls from one Remote Gateway 9150 station to another station on the same Remote Gateway 9150 unit) through the Remote Gateway 9150 unit when such calls are made on the host calling key. The signaling data is routed through the host PBX. However, the voice path is routed through the Remote Gateway 9150 unit to:<ul style="list-style-type: none">— prevent tromboning between the RLC and Remote Gateway 9150 unit— save connection bandwidth■ Click on the Disable option button to route the voice path for these calls through the PBX. The signaling data is routed through the host PBX. The default is Disable. <p>Note: You must enable the DN Discovery feature in order for the Local SwitchOver feature to work. Refer to the <i>Reach Line Card Installation and Administration Guide</i> (NTP 555-8421-210) to enable DN Discovery.</p>

Field	Description
Companding Algorithm	<p>A Companding Algorithm, or coding law, is a PCM standard for encoding an analog voice signal into a digital bit stream. There are two main coding laws in common use around the world, A-law and μ-law (Mu-law). A-law is the standard in Europe and most areas outside of North American influence, while the North American and Japanese standard is Mu-law.</p> <p>Select A-law or Mu-law if you want the Remote Gateway 9150 unit to override the Automatic default coding law.</p> <p>Valid options are Automatic, Mu-law, and A-law.</p> <p>Note: Automatic (coding law) is the default setting. When you choose Automatic, the Remote Gateway 9150 unit uses the coding law configured for the ISDN BRI module in use.</p> <p>For a listing of line types and their respective default coding laws, refer to “ISDN Line Type” on page 226.</p>
Multiple Subscriber Number	<p>Remote Gateway 9100 Series supports Multiple Subscriber Numbering (MSN), allowing you to configure each B-channel with a unique DN. If you do not have a unique DN for each B-channel, then the first B-channel you configure defines the number for both B-channels.</p> <ul style="list-style-type: none">■ Click on the Enable option button if the Central Office provides a unique DN for each individual B-channel.■ Click on the Disable option button if the Central Office provides one DN to be used for both B-channels. <p>The default is Enable.</p>
International Tones	<p>Click on the International Tones button to configure tones corresponding to your country on your Remote Gateway 9150 unit. Refer to “International tones support” on page 186 for a detailed description of the tones that you can configure using this setting.</p>

International tones support

International Tones support allows users to integrate Remote Gateway 9100 Series seamlessly into their existing telecommunications networks in countries that use tones different from North American tones, which are the defaults. Determine existing tone configurations for each field in the International Tone Support dialog box by accessing LD 56 through the switch administration terminal. The exact procedure for accessing LD 56 is available in documentation for your specific PBX.

The Tone Code field on the International Tones Support dialog box specifies the frequency and levels for the NT8D17 TDS card.

When configuring International Tones, consider the following:

- International Tone configuration uses NT8D17 card Tone Codes. These codes are valid for all countries and Meridian 1 PBX 11 or IPE Controller cards.
- To configure the four international tones, you need to obtain the following FTC values for DIAL, RGBK, BUSY and OVFL from LD 56 of your PBX:

```
>ld 56
REQ prt
TYPE FTC      Look for the DIAL,RGBK, BUSY and OVFL values.
...
DIAL
XTON 129      Enter the XTON value as the "Tone Code" value for this
XCAD 000      tone. XCAD is used below to determine the Repeat, No.
RGBK          of Cycles and Cadence Time.
XTON 132
XCAD 32
BUSY
XTON 130
XCAD 30
OVFL
XTON 130
XCAD 0
```


In the following example there are three different values for XCAD. Collect the LD 56 WCAD details for each different XCAD value.

```
>ld 56
REQ prt
TYPE FCAD
WCAD 0      for XCAD 0
CDNC 00000 00000 00000 00000 00000 00000 00000 00000 0000 00000
END OFF
WTON NO

REQ prt
WCAD 30
CDNC 100 50 00000 ...
END REPT
CYCS 1
WTON NO

REQ prt
WCAD 32
CDNC 102 102 205 819 00000 ...
END REPT
CYCS 1 2
WTON NO
```

Note the values printed for CDNC, END, and CYCS.

If END = REPT, then the value entered into the End Repeat field is “Repeat”.
CYCS usually has “1” or “1 2”. Enter the largest number as the No. of Cycles.
Enter the non-zero CDNC values into the Cadence Time fields.

Getting there 9150 → Configuration Manager → 9150 System Configuration

International Tones Support property sheet

The screenshot shows a Windows-style dialog box titled "International Tones Support". It contains the following controls:

- Tone Type:** A dropdown menu currently showing "DIAL".
- End Repeat:** Two radio buttons, "Off" (selected) and "Repeat".
- Tone Code:** A text input field containing the number "4".
- No of Cycles:** A text input field containing the number "0".
- Cadence Time:** A section with two rows of four empty text input fields each, for configuring timing intervals.
- Buttons:** "OK", "Close", "Default", and "Help" at the bottom.

Configuring International Tones

To configure International Tones:

- 1 Click on the **International Tones** button in the 9150 System Configuration property sheet.
- 2 Complete the fields as described in "International Tones field descriptions" on page 189.
- 3 Click on the **OK** button to save the information in the temporary work file.

Note: Refer to the Configuration Manager Help file for more information about International Tones.

International Tones field descriptions

Field	Description
Tone Type	<p>Tones inform users as to call status. Select the tone that you want to configure.</p> <p>Valid options are DIAL, RGBK, BUSY, and OVFL.</p> <p>DIAL – Dial tone signifies that the telephone is ready to receive dialed digits.</p> <p>RGBK – Ringback signifies that the dialed line is ringing.</p> <p>BUSY – Busy signal signifies that the dialed line is not ready to receive calls.</p> <p>OVFL – Overflow (congestion) tone signifies that there are no channels available.</p>
End Repeat	<ul style="list-style-type: none">■ Click on the Off option button if you want the tone type you selected to be a constant tone. <p>Note: If you chose End Repeat: Off, then the No of Cycles and Cadence Time fields are dimmed.</p> <ul style="list-style-type: none">■ Click on the Repeat option button if you want the selected tone type to have on and off phases. <p>The default is Off.</p>
Tone Code	<p>Enter the four-letter LD 56 Tone Code that you want this Remote Gateway 9150 unit to use for the tone type you selected.</p> <p>The default is 4.</p>

Field	Description
No of Cycles	<p>Enter the number of cycles that you want in the tone type you selected.</p> <p>Two fields in the Cadence Time field become active for each cycle you request. That is, they are no longer dimmed. The boxes turn white, signifying that you can enter information into that box. For example, if you choose 1 cycle, two boxes turn white. If you choose 3 cycles, six boxes turn white, and so on.</p> <p>Valid options are 1, 2, 3, and 4.</p>
Cadence Time	<p>Tones include on and off phases. One or more cycles of on and off phases make up a tone's cadence. For example, the default cadence for normal North American ringing is 2 seconds on, 4 seconds off, 2 seconds on, 4 seconds off, and so on. In the Cadence Time fields, enter the length, in milliseconds, of the phases of the cadence that you want to configure for the tone type you selected.</p> <p>Find the proper entries for the Cadence Time fields in the FTC: Flexible Tones and Cadences data block in the Prompts and Responses section of the <i>X11 Administration Guide</i> (NTP 553-3001-311).</p> <p>You can also calculate these entries using the formula in the following example, which calculates a phase of 2 seconds (2000 milliseconds [ms]):</p> <p>For 96 ms cadence increments:</p> $2000/96 = 20.83 = 21 \text{ (always round up)}$ $21 * 96 = 2016$ <p>multiple of 5 closest to 2016 = 2015</p> $2015 / 5 = 403$

Field	Description
Cadence Time (continued)	<p>For 128 ms cadence increments:</p> $2000/128 = 15.625 = 16$ $16 * 128 = 2048$ <p>multiple of 5 closest to 2048 = 2050</p> $2050 / 5 = 410$ <p>The shortcut is dividing the time by 5 (2000 ms / 5 = 400). To reverse the calculation, multiply the CDNC number by 5 (410 * 5 = 2050, 403 * 5 = 2015). This removes the need to know the actual software cadence increment value.</p>

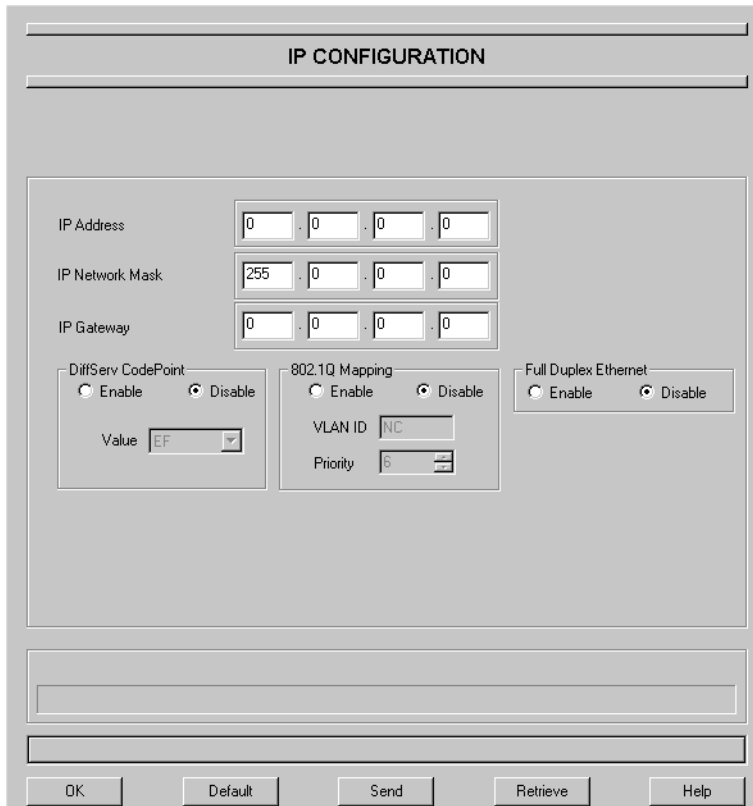
IP configuration

This section explains how to enter the IP address, subnet mask, and default gateway for the Remote Gateway 9150 unit.

Note: Even if you plan to route calls over the PSTN only, you must assign an IP address and gateway to the Remote Gateway 9150 unit and RLC to allow remote administration.

Getting there 9150 → Configuration Manager → IP Configuration

IP Configuration property sheet



The IP Configuration property sheet is a dialog box with a title bar labeled "IP CONFIGURATION". It contains several input fields and checkboxes for configuring network settings. The fields are organized into three rows: IP Address, IP Network Mask, and IP Gateway. Below these are three sections: DiffServ CodePoint, 802.1Q Mapping, and Full Duplex Ethernet. The DiffServ CodePoint section has radio buttons for Enable and Disable, and a Value dropdown menu set to EF. The 802.1Q Mapping section has radio buttons for Enable and Disable, a VLAN ID text box set to NC, and a Priority spinner box set to 6. The Full Duplex Ethernet section has radio buttons for Enable and Disable. At the bottom of the dialog are five buttons: OK, Default, Send, Retrieve, and Help.

IP CONFIGURATION				
IP Address	0	0	0	0
IP Network Mask	255	0	0	0
IP Gateway	0	0	0	0
DiffServ CodePoint		802.1Q Mapping		Full Duplex Ethernet
<input type="radio"/> Enable <input checked="" type="radio"/> Disable		<input type="radio"/> Enable <input checked="" type="radio"/> Disable		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Value: EF		VLAN ID: NC		
		Priority: 6		
OK Default Send Retrieve Help				

Configuring the IP addresses

To configure the IP addresses:

- 1 Complete the fields as described in “IP Configuration field descriptions” on page 193.
- 2 Click on the **OK** button.

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

- 3 Click on the **Send** button to update the Remote Gateway 9150 unit with the new information.

Notes:

- a. When you change IP configuration parameters and Save to Flash, calls can be dropped. Ensure that there are no active calls when you make changes to these parameters.
- b. To save changes to Flash memory, select Upload → Save to Flash from the Menu Bar.

IP Configuration field descriptions

Field	Description
IP Address	Enter the IP address of the Remote Gateway 9150 unit.
IP Network Mask	Enter the subnet mask of the currently logged-on Remote Gateway 9150 unit. The subnet mask identifies to the Remote Gateway 9150 unit which portion of the IP address represents the network and which portion represents the host.
IP Gateway	Enter the IP address of the IP gateway serving the Remote Gateway 9150 unit. A gateway is a device that functions as a node on two networks, forwarding packets from one network to addresses on the other networks. In Remote Gateway 9100 Series context, the gateway is the device on the network that directs traffic to and from the Remote Gateway 9150 unit.

Field	Description
DiffServ CodePoint	<p>This setting modifies the IP Header and is applicable across the entire WAN. If enabled, this feature allows you to set the DiffServ CodePoint value. Refer to the "DiffServ CodePoint: Value" for a list of values.</p> <ul style="list-style-type: none"> ■ Click on the Enable option button if you want to allow prioritization of voice packets sent from this Remote Gateway 9150 unit over WAN portions of the network. ■ Click on the Disable option button if you do not want to allow prioritization of voice packets sent from this Remote Gateway 9150 unit over WAN portions of the network. <p>The default is Disable.</p>
DiffServ CodePoint: Value	<p>Select the DiffServ CodePoint value from the drop down box. Valid options and their value (in hexadecimal) are:</p> <ul style="list-style-type: none"> ■ CS7 (Precedence 7 - Network Control) - 0x38 ■ CS6 (Precedence 6 - Inter-network Control) - 0x30 ■ EF (Expedited Forwarding) - 0x2E ■ AF41 (Assured Forwarding Class 4, Delay = Normal, Throughput = High, Reliability = Normal) - 0x22 ■ AF31 (Assured Forwarding Class 3, Delay = Normal, Throughput = High, Reliability = Normal) - 0x1A ■ AF21 (Assured Forwarding Class 2, Delay = Normal, Throughput = High, Reliability = Normal) - 0x12 ■ AF11 (Assured Forwarding Class 1, Delay = Normal, Throughput = High, Reliability = Normal) - 0x0A ■ DE (Default) - 0x00 <p>The default is EF.</p>

Field	Description
802.1Q Mapping	<p>This setting inserts an additional tag at the Media Access Control (MAC) layer of IEEE 802.3 and therefore ends at the first router. Refer to RFC 2474.</p> <ul style="list-style-type: none">■ Click on the Enable option button if you want to allow prioritization of voice packets sent from this Remote Gateway 9150 unit over LAN portions of the network.■ Click on the Disable option button if you do not want to allow prioritization of voice packets sent from this Remote Gateway 9150 unit over LAN portions of the network. <p>The default is Disable.</p>
802.1Q Mapping: VLAN ID	<p>Enter the Virtual Local Area Network (VLAN) ID for 802.1Q Mapping.</p> <p>Valid entries are 0 through 4094 (0xFFE) and NC (Not Configured).</p> <p>The default is NC.</p>
802.1Q Mapping: Priority	<p>Select the priority value for 802.1Q Mapping from the Priority scroll box.</p> <p>Valid options are 0 through 7.</p> <p>The default is 6.</p>

Field	Description
Full Duplex Ethernet	<p>This setting configures Ethernet support on the Remote Gateway 9150 unit vintages AD, BD, CD, and later to allow simultaneous transmission and reception of Ethernet packets. When you enable full-duplex Ethernet, you must also set the corresponding port on the connected switch, hub, or router to 10 FULL Duplex. With full-duplex Ethernet enabled, the Remote Gateway 9150 unit's Ethernet collision LED remains on solid (constantly lit). Remote Gateway 9100 Series products do not support Auto negotiation of the Ethernet interface.</p> <ul style="list-style-type: none">■ Click on the Enable option button if you want to allow 10-Megabyte transmission in both directions, send and receive.■ Click on the Disable option button if you do not want to allow 10-Megabyte transmission in both directions, send and receive. <p>Note: When you configure a full-duplex Ethernet connection, the Remote Gateway 9150 unit's Ethernet collision LED remains on solid (constantly lit).</p> <p>The default is Disable.</p>

Prioritizing voice traffic over shared networks

Prioritizing voice traffic on shared networks can improve QoS on LAN and WAN segments of the network that support prioritization. Achieving the desired QoS through prioritization over LAN connections requires you to enable 802.1Q Mapping. Achieving the desired QoS through prioritization over WAN connections requires you to enable the DiffServ CodePoint.

For more information on DiffServ, 802.1Q, and quality of service in general, refer to “Evaluating your network”, and “Quality of service issues” in the *Remote Gateway 9100 Series Network Engineering Guidelines* (NTP 555-8421-103).

RLC connection configuration

This section describes how to configure information needed by the Remote Gateway 9150 unit to establish connections with the RLC on the host PBX.

Getting there 9150 → Configuration Manager → RLC Connection Configuration

RLC Connection Configuration property sheet

RLC CONNECTION CONFIGURATION

Unit ID:

IP Connection

☐ Enable ☒ Disable

IP Address:

IP Signaling: ☐ Permanent ☒ On Demand

PSTN Connection

☐ Enable ☒ Disable

PSTN Number to Connect to RLC:

Block Incoming Local Call on Primary B Channel: ☒ Enable ☐ Disable

Security Level:

Security Id: Inbound Security ID Outbound Security ID

Caller ID...

Configuring the RLC connection information

To configure the RLC connection information:

- 1 Complete the fields as described in “RLC Connection Configuration field descriptions” on page 203.
- 2 Click on the **OK** button
- 3 Click on the **Send** button to update the Remote Gateway 9150 unit with the new information.

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

Note: To save changes to the Remote Gateway 9150 unit's Flash memory, select Upload → Save to Flash from the Menu Bar.

PSTN connection configuration

The PSTN number configured on this property sheet corresponds to the dedicated network port on the RLC for your Remote Gateway 9150 unit. The PSTN number to connect to the RLC must be configured in a specific manner. If you select Caller ID as the security level, then the PSTN number that you enter for the Remote Gateway 9150 unit to connect to the RLC is compared with the telephone number configured on the RLC for your site. If the two numbers do not match, the call is dropped.

Note: Enter the PSTN number to connect to RLC exactly as it must be dialed by the Remote Gateway 9150 unit, including 1 for long distance and 9 for Centrex trunk access.

Permanent PSTN connection

When using multiple Remote Gateway 9100 Series units, you must only configure the permanent PSTN connections for the RLC's primary network ports. If you only use one Remote Gateway 9100 Series unit, you can use additional permanent PSTN connections.

Configuring the PSTN number

To configure the PSTN number:

- 1 Enable the PSTN Connection option.
- 2 Enter the telephone that the Remote Gateway 9150 unit will dial to connect to the RLC in the PSTN Number to Connect to RLC field.
- 3 Click on the **OK** button

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

- 4 Click on the **Send** button to update the Remote Gateway 9150 unit with the new information.

Note: To save changes to the Remote Gateway 9150 unit's Flash memory, select Upload → Save to Flash from the Menu Bar.

Security level configuration

It is recommended that you implement a security authentication method on both the RLC and the Remote Gateway 9150 unit to prevent toll fraud.

The security level defines what type of security authentication is used between the Remote Gateway 9150 unit and the host PBX. The information used to perform security authentication depends on the security level chosen. There are three levels of security:

- No security (default setting)
- Caller ID
- Provision ID

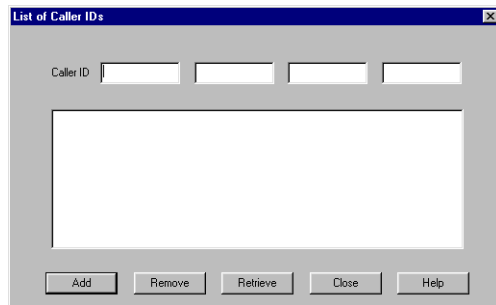
For a detailed description of these security levels refer to “System security” on page 12.

Configuring the security level

To configure the security level:

- 1 Select one of the following security level settings from the Security Level list box:
 - No Security
 - Caller ID
 - Provision ID
- 2 If you selected Caller ID or Provision ID security levels, do one of the following:

IF you selected	THEN
Caller ID,	click on the CallerID button. Result: The List of Caller IDs dialog box displays.



In the Caller ID field, enter the telephone number that is permitted to call the Remote Gateway 9150 unit. Ensure that the telephone number you enter matches the Caller ID actually presented by the RLC.

Click on the **OK** button, and then click on the **Add** button from the pop-up menu that displays.

Result: The telephone number displays in the blank field.

IF you selected	THEN
Provision ID,	<p>the Security ID fields are enabled.</p> <p>Do the following:</p> <ul style="list-style-type: none">■ Enter the RLC's security identifier (must be a 10 digit password) in the Inbound Security ID field.■ Enter the Remote Gateway 9150 unit's security identifier (must be a 10 digit password) in the Outbound Security ID field. <p>Note: You must configure the same security identifiers in reverse on the RLC port associated with this Remote Gateway 9150 unit.</p>
3	<p>Click on the OK button</p> <p>Result: Configuration Manager writes the changes to a temporary file on the administration PC.</p>
4	<p>Click on the Send button to update the Remote Gateway 9150 unit with the new information.</p> <p>Note: To save changes to the Remote Gateway 9150 unit's Flash memory, select Upload → Save to Flash from the Menu Bar.</p>

RLC Connection Configuration field descriptions

Field	Description
Unit ID	The RLC's non-configurable Unit ID is 254.
IP Connection	<ul style="list-style-type: none">■ Click on the Enable option button if you want to route calls over your IP network.■ Click on the Disable option button if you do not want to route calls over your IP network. <p>The default is Disable.</p>
PSTN Connection	<p>Click on the Enable option button if you want to route calls over the PSTN.</p> <p>Click on the Disable option button if you do not want to route calls over the PSTN.</p> <p>The default is Disable.</p>
IP Address	<p>Enter the RLC's IP address.</p> <p>The Remote Gateway 9150 unit uses this IP address to connect to the RLC over the IP network.</p> <p>Note: If you disable the IP connection, these fields are dimmed.</p>
PSTN Number to Connect to RLC	<p>If you enabled the PSTN connection, enter the telephone number used to connect to the RLC.</p> <p>If you want, you can also include the following characters in the telephone number:</p> <ul style="list-style-type: none">■ a period (.) for a caller ID separator■ a comma (,) for a delay of 1/2 second■ a dash (-) for a null separator <p>Note: Enter the PSTN number to connect to RLC exactly as it must be dialed by the Remote Gateway 9150 unit, including 1 for long distance and 9 for Centrex trunk access.</p>

Field	Description
IP Signaling	<ul style="list-style-type: none">■ Click on the Permanent option button if you want the signaling link to the Remote Unit to never close. Note: This is useful in times when the Remote unit is behind a NAT router.■ Click on the On Demand option button if you want the signaling link to close once there are no active calls between the RLC and the Remote unit. <p>The default is On Demand.</p> <p>Note: If you disable the IP connection, these option buttons are dimmed.</p> <p>Refer to “Deployment options” on page 75 for more information.</p>
Block Incoming Local Call on Primary B Channel	<ul style="list-style-type: none">■ Click on the Enable option button if the primary B-channel (trunk) <i>should not</i> receive incoming local calls.■ Click on the Disable option button if the primary B-channel (trunk) <i>should</i> receive incoming local calls. <p>The default is Enable.</p>

Field	Description								
Security Level	Select the security level that you want to assign to the Remote Gateway 9150 unit according to the following table: <table><tr><th>Level</th><th>Description</th></tr><tr><td>No Security</td><td>When set to security level 1, the Remote Gateway 9150 permits all incoming calls regardless of source. Note: No security is the default security level.</td></tr><tr><td>Caller ID</td><td>When you select Caller ID, you can define the valid Caller IDs that the Remote Gateway 9150 can receive. If the Caller ID on the incoming call matches what is configured on the remote unit, the connection is established. If it does not match, the RLC drops the call. Note: Caller ID authentication cannot be performed over the IP network. Caller ID authentication can be used only on the PSTN.</td></tr><tr><td>Provision ID</td><td>If you select Provision ID, security identifiers must be configured on both the Remote Gateway 9150 and the RLC port that the unit is assigned to. When a connection to or from the host PBX is attempted, the security identifiers are compared. If they match, the connection is established. If they do not match, the call is dropped.</td></tr></table>	Level	Description	No Security	When set to security level 1, the Remote Gateway 9150 permits all incoming calls regardless of source. Note: No security is the default security level.	Caller ID	When you select Caller ID, you can define the valid Caller IDs that the Remote Gateway 9150 can receive. If the Caller ID on the incoming call matches what is configured on the remote unit, the connection is established. If it does not match, the RLC drops the call. Note: Caller ID authentication cannot be performed over the IP network. Caller ID authentication can be used only on the PSTN.	Provision ID	If you select Provision ID, security identifiers must be configured on both the Remote Gateway 9150 and the RLC port that the unit is assigned to. When a connection to or from the host PBX is attempted, the security identifiers are compared. If they match, the connection is established. If they do not match, the call is dropped.
Level	Description								
No Security	When set to security level 1, the Remote Gateway 9150 permits all incoming calls regardless of source. Note: No security is the default security level.								
Caller ID	When you select Caller ID, you can define the valid Caller IDs that the Remote Gateway 9150 can receive. If the Caller ID on the incoming call matches what is configured on the remote unit, the connection is established. If it does not match, the RLC drops the call. Note: Caller ID authentication cannot be performed over the IP network. Caller ID authentication can be used only on the PSTN.								
Provision ID	If you select Provision ID, security identifiers must be configured on both the Remote Gateway 9150 and the RLC port that the unit is assigned to. When a connection to or from the host PBX is attempted, the security identifiers are compared. If they match, the connection is established. If they do not match, the call is dropped.								

Field	Description
Security Id: Inbound Security ID	<p>If you selected Provision ID as the security level, enter the Security ID for incoming calls.</p> <p>This ID must be a 10-digit password. The Remote Gateway 9150 unit compares the security ID of the incoming call to the Inbound Security ID that is configured in this field. If the security IDs do not match, the Remote Gateway 9150 unit rejects the call.</p>
Security Id: Outbound Security ID	<p>If you selected Provision ID as the security level, enter the Security ID for outgoing calls.</p> <p>This ID must be a 10-digit password. The Remote Gateway 9150 unit sends the outbound security ID to the RLC. The RLC compares this ID to the configured Outbound Security ID that it has for this remote unit. If the security IDs do not match, the RLC rejects the call.</p>
Caller ID	<p>Click on the Caller ID button to configure the DN of the network port dedicated for connections to this Remote Gateway 9150 unit. When the RLC calls the Remote Gateway 9150 unit, it sends its Caller ID to the 9150 unit. The Remote Gateway 9150 unit compares the caller ID with the list of Caller IDs configured, and, if it does not find a match, it rejects the call.</p>

9150 port configuration

To place and receive calls, you must use Configuration Manager to configure each station (telephone or other device such as a fax machine) in your office.

Note: To ensure that digital telephones, ATAs, and MCAs operate as expected, you must specify the Phone Type when configuring a station as Local or Remote.

Getting there 9150 → Configuration Manager → 9150 Port Configuration

9150 Port Configuration property sheet

Ports 0 - 15 | Ports 16 - 31 | Ports 32 - 47 | Ports 48 - 64 |

9150 PORT CONFIGURATION

Port Type			RLC Port	Description		
Ports 0-15						
0	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	0	Phone Type: M2616 ,Add on Module 1	Configure
1	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	1	Phone Type: M2616 ,Add on Module 1	Configure
2	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	2	Phone Type: M2616 ,Add on Module 1	Configure
3	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	3	Phone Type: M2616 ,Add on Module 1	Configure
4	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	4	Phone Type: M2616 ,Add on Module 1	Configure
5	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	5	Phone Type: M2616 ,Add on Module 1	Configure
6	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	6	Phone Type: M2616 ,Add on Module 1	Configure
7	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	7	Phone Type: M2616 ,Add on Module 1	Configure
8	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	8	Phone Type: M2616 ,Add on Module 1	Configure
9	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	9	Phone Type: M2616 ,Add on Module 1	Configure
10	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	10	Phone Type: M2616 ,Add on Module 1	Configure
11	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	11	Phone Type: M2616 ,Add on Module 1	Configure
12	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	12	Phone Type: M2616 ,Add on Module 1	Configure
13	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	13	Phone Type: M2616 ,Add on Module 1	Configure
14	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	14	Phone Type: M2616 ,Add on Module 1	Configure
15	<input type="radio"/> Local	<input checked="" type="radio"/> Remote	<input type="radio"/> Local & Remote	15	Phone Type: M2616 ,Add on Module 1	Configure

OK Default Send Retrieve Get DN List Help

Configuring stations

To configure stations:

- 1 Locate the port that you want to configure by clicking on the appropriate port range tab, and then scrolling down the list.

The following table describes port number ranges and how they can be configured:

Ports	Can be assigned to
0–15 and 32–47	digital telephones. Note: The associated ports on the host PBX must be configured with voice capability.
16–31 and 48–63	stations equipped with ATAs or MCAs. Note: The associated ports on the host PBX must be configured with data capability.
64	a fax machine or other analog device (without an ATA). Note: The associated port on the host PBX must be configured with voice capability.

Note: You can use ports 32 through 47 and 48 through 63 only if this Remote Gateway 9150 unit connects to a 2-slot RLC on the host PBX.

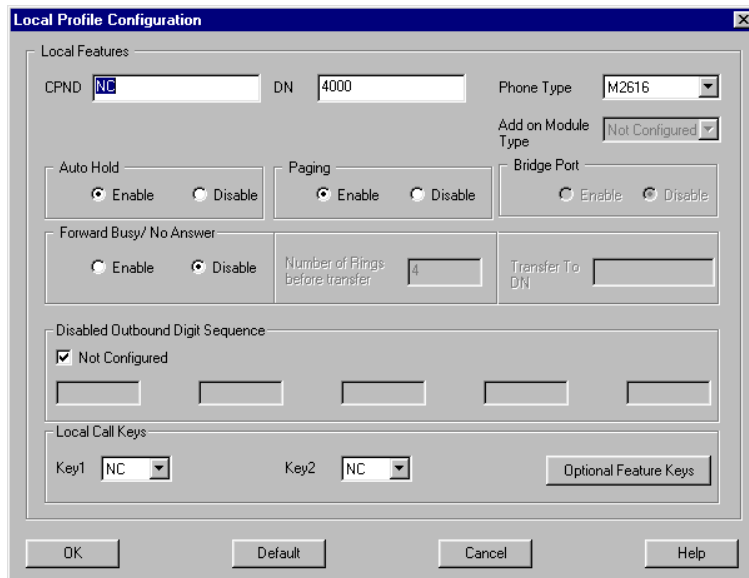
- 2 Under Port Type, click on the option button of the call processing capability that this station is to have:
 - Local: if only calls through the local PSTN are allowed. This option enables the Configure button for this port.
 - Remote: if only calls through the host PBX are allowed.
 - Local and Remote: if both local and remote calls and local station-to-station calling are allowed. This option enables the Configure button for this port so you can configure local station features and keys.
Note: Choose Local and Remote if you want to define a Bridge Port.
- 3 Accept the default RLC Port associated with this station, or enter a new RLC port number.

Exception: Do not associate a local-only port with an RLC port.

Notes:

- Generally, choosing matching Remote Gateway 9150 and RLC port numbers simplifies configuration and administration.
 - If the station is equipped with an MCA or ATA for data transmission, the RLC port must be configured on the host PBX with data capability.
- 4 If you selected Local or Local & Remote, click on the **Configure** button for the port you are configuring.

Result: The Local Profile Configuration dialog box displays.



The image shows a 'Local Profile Configuration' dialog box with the following fields and controls:

- Local Features:**
 - CPND:
 - DN:
 - Phone Type:
 - Add on Module Type:
- Auto Hold:** ☒ Enable ☐ Disable
- Paging:** ☒ Enable ☐ Disable
- Bridge Port:** ☐ Enable ☒ Disable
- Forward Busy/ No Answer:**
 - ☐ Enable ☒ Disable
 - Number of Rings before transfer:
 - Transfer To DN:
- Disabled Outbound Digit Sequence:**
 - ☒ Not Configured
 -
 -
 -
 -
 -
- Local Call Keys:**
 - Key1:
 - Key2:
 -

Buttons at the bottom:

- 5 Complete the fields as described in “Local Profile Configuration field descriptions” on page 210.
- 6 Once you have completed the Local Profile Configuration, click on the **OK** button.

Result: The 9150 Device Configuration property sheet re-displays. The configurations you set are displayed in the port’s Description field.

Local Profile Configuration field descriptions

Field	Description
CPND	<p>Enter the Calling Party Name Display (CPND) for the user assigned to the station.</p> <p>The default is NC (Not Configured).</p>
DN	<p>Enter the user's local extension number.</p> <p>Note: If Auto DN Discovery is enabled on the RLC, then this field is configured to be the same DN as the primary DN configured on the host PBX for this station.</p>
Phone Type	<p>Select the telephone model type connected to the port.</p> <p>Valid options are M2006, M2008, M2216, M2616, M2616CT, M3110, M3310, M3820, M3901, M3902, M3903, M3904, M3905, MCA, ATA, and Other.</p> <p>The default is M2616.</p>
Add on Module Type	<p>Select the applicable Add on Module for the M3904 and M3905 telephones.</p> <p>Valid options are Not Configured, KBA, and DBA.</p> <p>The default is Not Configured.</p>
Auto Hold	<ul style="list-style-type: none">■ Click on the Enable option button if active calls are to be automatically put on hold when another call appearance key is pressed.■ Click on the Disable option button if active calls are to be disconnected when another call appearance key is pressed. <p>The default is Enable.</p>
Paging	<ul style="list-style-type: none">■ Click on the Enable option button if this station is to be allowed to announce pages.■ Click on the Disable option button if this station is not to be allowed to announce pages. <p>The default is Enable.</p>

Field	Description
Bridge Port	<ul style="list-style-type: none">■ Click on the Enable option button to give inbound PSTN calls access to certain PBX features.■ Click on the Disable option button if you want to support a telephone on this port. <p>The default is Disable.</p> <p>Notes:</p> <ul style="list-style-type: none">■ When configuring Local-only ports on a Remote Gateway 9150 unit, the Bridge Port setting is not available.■ If a Remote Gateway 9150 unit port is configured with Bridge Port enabled, do not attach a telephone set to this port.■ For a telephone set connected to a Remote Gateway 9150 unit with Local and Remote capability, the Bridge Port does not need to be enabled to allow you to have access to Bridge Port features.
Forward Busy/No Answer	<ul style="list-style-type: none">■ Click on the Enable option button to allow incoming calls to this station to be forwarded if they are not answered by the number of rings configured in the Number of Rings before transfer field or if the station is busy.■ Click on the Disable option button if calls are not to be forwarded. <p>The default is Disable.</p>
Forward Busy/No Answer: Number of Rings before transfer	<p>Enter the number of times this station rings before transferring the call to the configured DN.</p> <p>Note: You must Enable Forward Busy/No Answer to configure this setting.</p> <p>The default is four rings.</p>

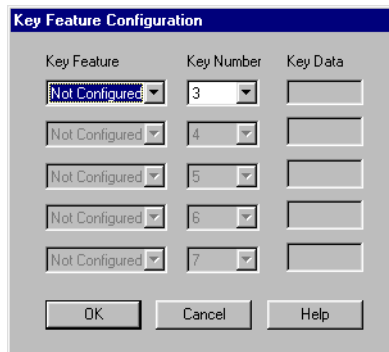
Field	Description
Forward Busy/No Answer: Transfer to DN	<p>Enter the DN where calls to this station are to be transferred if not answered before the configured number of rings.</p> <p>Note: This DN may be for a voicemail service or the DN of another station. You must Enable Forward Busy/No Answer to configure this setting.</p>
Disabled Outbound Digit Sequence	<p>Click on the Not Configured checkbox to enable these fields.</p> <p>This allows you to prevent this station from making certain type of calls. To prevent these types of calls, enter the digits that normally allow the calls to proceed.</p> <p>Example: Enter 1976 to prevent calls to 1-976 numbers.</p> <p>Note: You can configure five digit sequences. In order for calls to be restricted, the dialed number must contain a matching string at the beginning of the number.</p>
Local Call Keys (Key 1 and Key 2)	<p>The number selected identifies the feature key position on the telephone. Select the feature key you want to use for each local call appearance key.</p> <p>Note: If the port is configured as local and remote, Nortel recommends that you use keys 8 and 9 and that you do not use Key 0. You can select Key 0 if the port is configured as local only.</p> <p>Valid options are 0 through 75, and NC (Not Configured).</p> <p>The default is NC.</p>

Field	Description
-------	-------------

Optional Feature Keys

If you configured the port as Local, click on the **Optional Feature Keys** button to assign local features to specific keys.

Result: The Key Feature Configuration dialog box displays.



The dialog box is titled "Key Feature Configuration". It contains three columns: "Key Feature", "Key Number", and "Key Data".

Key Feature	Key Number	Key Data
Not Configured	3	
Not Configured	4	
Not Configured	5	
Not Configured	6	
Not Configured	7	

At the bottom are three buttons: OK, Cancel, and Help.

Note: Ensure that the selected key does not already have a feature assigned to it through the PBX.

■ Key Feature

Select the name of the feature you want to configure on this key.

Valid options are Call Transfer, Call Forward, Auto Dial, Make Set Busy, and Not Configured.

■ Key Number:

The key number identifies the feature key position on the telephone. Select the key you want for the feature you are configuring.

Note: If the station is configured as Local and Remote, the key number selected for the feature must match the feature key position defined in the PBX voice port configuration.

Valid options are 0 through 15.

■ Key Data

Enter the DN to be used by the feature, if applicable.

Bridge Ports

Bridge Ports provide integration between the host PBX dialing plan and the Remote Gateway 9150 unit local dialing plan. To determine the correct Bridge Port configuration for your particular Remote Gateway 9100 Series network, you must first consider the resource usage of both the Remote Gateway 9150 unit and RLC. The examples on pages 216 through 219 illustrate the most common resource usage scenarios in a Remote Gateway 9100 Series network. Configure a Bridge Port TN on the host PBX as a voice port. For further information, refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Terminology

In the following configuration examples, a local call is defined as a call that terminates on a Local Calling key of a digital telephone set connected to a Remote Gateway 9150 unit. This call can be from another local user, or an inbound call from the PSTN through the BRI circuits on the Remote Gateway 9150 unit. The primary DN is the first key on the digital telephone set connected to Remote Gateway 9150 unit that has a DN provided by the host PBX.

Notes:

1. Bridge Ports use the remote PBX DNs of Local and Remote digital telephone sets connected to Remote Gateway 9150 units to transfer local calls to the host PBX or to conference host PBX calls to local calls. At least one remote PBX line key must be idle for the Bridge Port to function properly.
2. You must ensure that both sides of the connection release when the calling party terminates a call on a Bridge Port in order for the Bridge Port to release.

Configuration scenarios

The following configuration scenarios show options for enabling conference and voice mail functionality at remote locations through Remote Gateway 9100 Series' Bridge Port feature.

Local inbound calls ring on digital telephone sets connected to a Remote Gateway 9150 unit and can be forwarded or conferenced to the host PBX through the following configuration:

- 1 Configure and enable DN Discovery on the RLC.

Note: DN Discovery replaces the DN configured on the Local Calling key of each digital telephone set connected to a Remote Gateway 9150 unit with the DN configured for the first call-capable key programmed for that digital telephone set on the host PBX, such as Key 0 or Key 1.

- 2 Configure the Local Calling keys of each digital telephone set connected to a Remote Gateway 9150 unit as required.

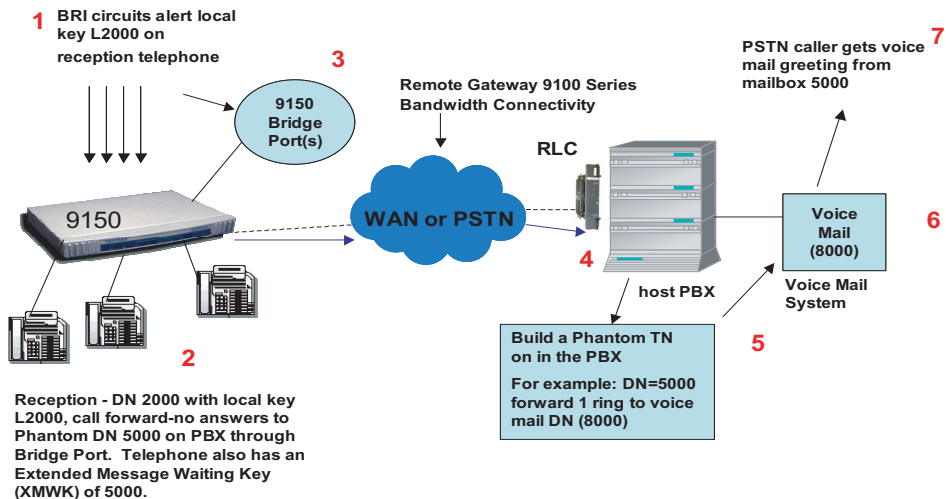
Note: One MADN can only appear as a local key on one digital telephone set connected to a given Remote Gateway 9150 unit. All other appearances of this MADN on digital telephone sets connected to that same Remote Gateway 9150 unit must be as host keys.

- 3 Configure the BRI trunk groups to alert the required local DNs when inbound calls are received on the BRI lines.
- 4 Configure enough Bridge Ports to provide the level of call blocking desired. For example, if four inbound BRI calls are forwarded to the host PBX then you require four Bridge Ports.
- 5 Review the DSP channel requirements. Each Bridge Port call requires a DSP channel and the associated bandwidth.

When a local call is presented and answered on a digital telephone set connected to a Remote Gateway 9150 unit, you can then press the Transfer (or Conference) key. The call indicator of the primary DN key then lights, you hear a host PBX dialtone, and you can proceed to dial.

Note: Your primary DN is used to conference a local call. The Bridge Port connects the local user to the host PBX, the Remote Gateway 9150 unit connects your primary DN to the host PBX, and the Conference feature on the host PBX ties it all together.

Scenario 1

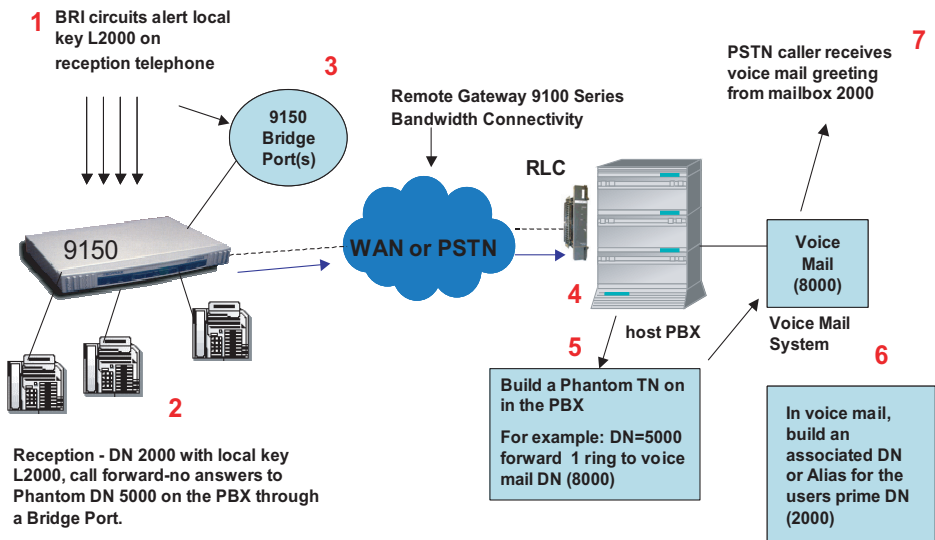


The reception digital telephone set (L2000) answers all local BRI calls. Calls that are not answered use a Bridge Port to transfer to a dedicated remote site voice mailbox for the entire Remote Gateway 9150 unit.

- Local BRI calls ring the local key(s) of a reception telephone (L2000).
- These calls, when unanswered, call forward-no answer according to the Remote Gateway 9150 unit's 9150 Port Configuration property sheet settings to a PBX Phantom TN (5000).
- This PBX Phantom TN forwards after one ring to the voice mail target DN (8000).
- A designated mailbox, such as mailbox number 5000, is built in voice mail.
- An Extended Message Waiting Key (XMWK) of 5000 on the reception telephone notifies the user of voice mail messages left from Remote Gateway 9150 unit BRI calls.

Note: An XMWK can be added to any or all digital telephone sets attached to a Remote Gateway 9150 unit.

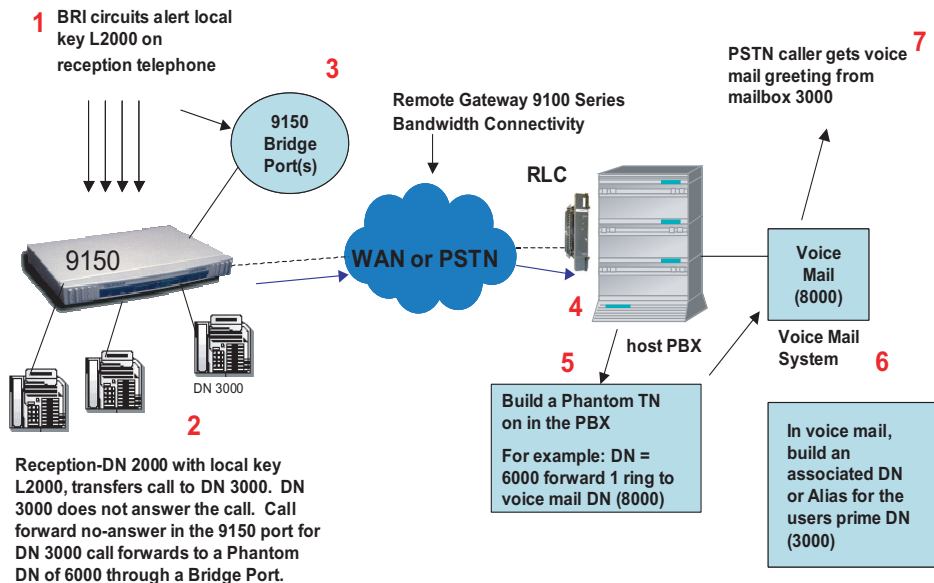
Scenario 2



All calls alert the reception telephone local key (L2000). Unanswered calls transfer to the receptionists personal voice mailbox (2000).

- Local BRI calls ring the local keys of a reception telephone (4000).
- These calls, when unanswered, call forward-no answer according to the Remote Gateway 9150 unit's 9150 Port Configuration property sheet settings to a PBX Phantom TN (5000).
- This PBX Phantom TN forwards after one ring to the voice mail target DN (8000).
- The voice mail system has a mailbox for DN 2000. You must add an "Alias" (Octel Terminology) or "Associated/Extension DN" (Meridian Terminology) of 5000 to the DN mailbox for 2000.
- Once this call arrives in voice mail, the "Alias" or "Associated/Extension DN" sends this PSTN call to the personal voice mailbox for DN 2000.

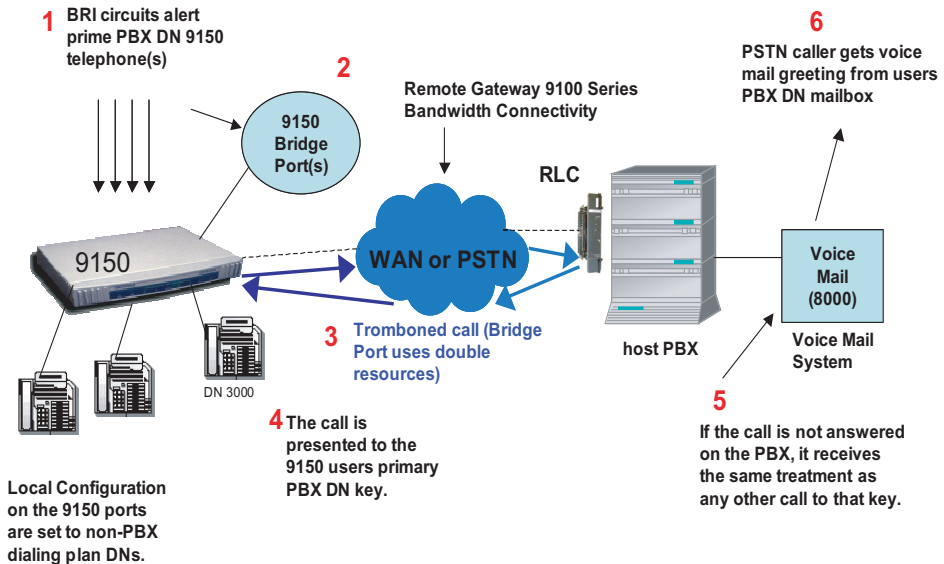
Scenario 3



All calls alert the reception telephone local key (L2000). The receptionist answers these calls and then transfers them to other DN's on the Remote Gateway 9150 unit. If the calls are not answered after the transfer, the calls are placed in that user's personal voice mailbox.

- Local BRI calls ring the local keys of a reception telephone (L2000).
- When answered, these calls transfer to other DN's on the Remote Gateway 9150 unit (3000).
- The user at DN 3000 is away and this call transfers to the user's personal voice mailbox.
- This port in 9150 Port Configuration or DN 3000 is enabled to call forward-no answer to a Phantom DN (6000) configured in the PBX.
- This PBX Phantom TN forwards after one ring to the voice mail target DN (8000).
- The voice mail system has a mailbox for DN 3000. You must add an "Alias" (Octel Terminology) or "Associated/Extension DN" (Meridian Terminology) of 6000 to the DN mailbox for 3000.
- Once this call arrives in voice mail, the "Alias" or "Associated/Extension DN" sends this PSTN call to DN 3000 personal voice mailbox.

Scenario 4



All local inbound calls pass immediately to the host PBX and then are “trombone” re-directed to the Remote Gateway 9150 unit’s user’s primary PBX DN key.

ATTENTION!

This scenario creates tromboning on every call and uses double DSP and bandwidth resources. Not only does this trombone add additional delay but you **MUST** also ensure that the DSP and bandwidth resources allow for this situation. The dual encoding of voice calls causes further degradation of voice quality, which can be unacceptable to some users. Additionally, with DN Discovery disabled, Local Switchover cannot be used. Therefore, all calls within the Remote Gateway 9150 unit’s local office require DSP and bandwidth resources.

- Disable DN Discovery. This forces the Remote Gateway 9150 unit to use local DNs (non-PBX DNs) and does not replace the local DN with the primary PBX DN.
- Configure enough Bridge Ports to provide the desired level of call blocking. For example, four inbound BRI calls forwarded to the host PBX require four Bridge Ports.

- Ensure that the DNs configured for the Remote Gateway 9150 unit's local ports are not the same as any host PBX DNs.
- On Configuration Manager's Trunk Group Configuration property sheet, configure the user's primary PBX DN in one of the Local DN to Alert fields.

Note: This configuration provides a local presence for a Remote Gateway 9150 unit user while maintaining full usage of the host PBX voice mail resources. For example, an office can publish one of the BRI DNs (such as, 555-1212) as a direct number. Calls to this DN alert the user's Remote Gateway 9150 unit digital telephone set. They pass from the BRI to the Bridge Port, trombone to the host PBX, then to the primary DN on the user's digital telephone set. If the digital telephone set is busy, regular call treatment occurs, including directing the call to the user's voice mailbox.

Analog port

The analog port (port 64) on a Remote Gateway 9150 unit is intended to provide intra-office support according to these conditions:

- The port provides the basic functionality of a POTS line, such as:
 - dial tone
 - DTMF tones
 - local ringback
 - other standard tones
 - ring trip voltage for ringing a telephone or a fax machine
- The port does not provide the following functionalities:
 - disconnect supervision
 - hook switch flash
 - Message Waiting functionality

To make and receive local calls on the analog port or an ATA configured to a Local and Remote port, configure a local DN to that port. You must then include that port in a trunk group for it to receive inbound voice or fax calls. To place an outbound voice or fax call on this port, you must enter the Local Calling SPRE Code to obtain a local dial tone.

Because an analog port does not have disconnect supervision, a user must place the device connected to that port on-hook to end a call. If the user does not place the device connected to the analog port on-hook to end a call, it does not ring for subsequent calls.

Configuring a fax station

The Remote Gateway 9150 unit provides the ability to connect and use a fax machine. You can define port 64 as the fax machine on the Remote Gateway 9150 unit in one of the following ways:

TO allow all fax calls to be made or received through

the local PSTN only,	define the fax machine as a local device.
the host PBX,	define the fax machine as a remote device.
both the local PSTN and the host PBX,	define the fax machine as a local and remote device.
	To place a local fax call on a Local and Remote port, you must first enter the Local Calling SPRE Code. The default Local Calling SPRE Code is #8.

Note: When faxes are sent and received through the host PBX, they are sent uncompressed (that is, they require 64 Kbps of bandwidth).

For instructions on configuring the fax port, refer to “Configuring the fax port” on page 222.

For instructions on configuring a trunk group that rings only on the fax machine, refer to “To configure trunk groups:” on page 236.

Configuring the fax port

To configure the fax port:

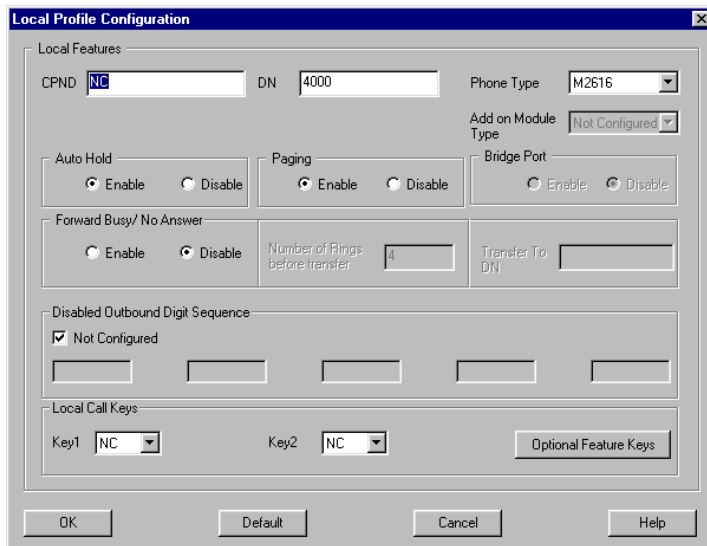
- 1 Locate port 64.
- 2 On port 64, under Port Type, click on the option button of the call processing capability the fax machine is to have:
 - Local: if only faxes through the local PSTN are allowed. This option enables the Configure button for this port.
 - Remote: if only faxes through the host PBX are allowed.
 - Local and Remote: if both local and remote faxing are allowed. This option enables the Configure button for this port so you can configure local station features and keys.
- 3 Accept the default RLC Port assigned to this station, or enter a new RLC port number.

Notes:

- Generally, choosing matching Remote Gateway 9150 and RLC port numbers simplifies configuration and administration.
- For fax transmissions, the RLC port must be configured on the host PBX with voice capability.

- 4 If you selected Local or Local & Remote, click the **Configure** button for the port you are configuring.

Result: The Local Profile Configuration dialog box displays.



The image shows the 'Local Profile Configuration' dialog box. It has a title bar with the text 'Local Profile Configuration' and a close button. The dialog is divided into several sections. The 'Local Features' section contains fields for 'CPND' (set to 'NC'), 'DN' (set to '4000'), 'Phone Type' (set to 'M2616'), and 'Add on Module Type' (set to 'Not Configured'). Below these are three groups of radio buttons: 'Auto Hold' (Enable/Disable), 'Paging' (Enable/Disable), and 'Bridge Port' (Enable/Disable). The 'Forward Busy/ No Answer' section has 'Enable' and 'Disable' radio buttons, a 'Number of Rings before transfer' field (set to '4'), and a 'Transfer To DN' field. The 'Disabled Outbound Digit Sequence' section has a checked 'Not Configured' checkbox and five empty text boxes. The 'Local Call Keys' section has 'Key1' and 'Key2' dropdown menus (both set to 'NC') and an 'Optional Feature Keys' button. At the bottom are 'OK', 'Default', 'Cancel', and 'Help' buttons.

- 5 In the Local Features: CPND field, enter a description (for example, FAX).
- 6 Enter the number used to ring the fax machine in the Local Features: DN field.
- 7 Click on the **Disable** option button under Local Features for the following:
 - Auto Hold
 - Forward Busy/No Answer
 - Paging
 - Bridge Port (Local and Remote only)
- 8 If applicable, enter the digits that prevent a certain type of call from proceeding in the Disabled Outbound Digit Sequence field.
- 9 Specify the positions of the Local Call Keys.

Note: Key 0 is not recommended for ports defined as Local and Remote. Keys 8 and 9 are recommended. You can select Key 0 if the port is configured as local only.

- 10** Click on the **OK** button

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

- 11** Click on the **Send** button to update the Remote Gateway 9150 unit with the new information.

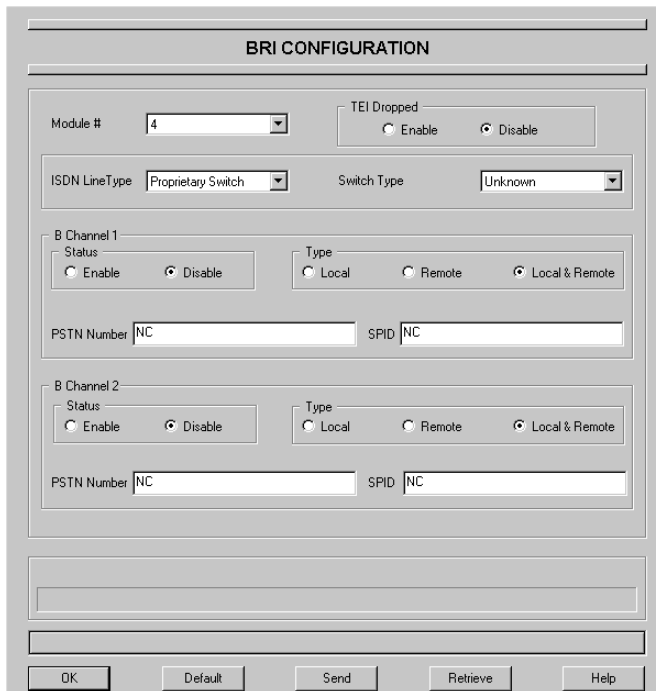
Note: To save changes to the Remote Gateway 9150 unit's Flash memory, select Upload → Save to Flash from the Menu Bar.

BRI configuration

This topic shows you how to configure the BRI trunks. Refer to “Trunk group configuration” on page 232 for a detailed explanation of BRI configuration settings.

Getting there 9150 → Configuration Manager → BRI Configuration

BRI Configuration property sheet



The image shows a 'BRI CONFIGURATION' dialog box with the following fields and controls:

- Module #**: A dropdown menu with the value '4' selected.
- TEI Dropped**: Radio buttons for 'Enable' and 'Disable', with 'Disable' selected.
- ISDN LineType**: A dropdown menu with 'Proprietary Switch' selected.
- Switch Type**: A dropdown menu with 'Unknown' selected.
- B Channel 1**:
 - Status**: Radio buttons for 'Enable' and 'Disable', with 'Disable' selected.
 - Type**: Radio buttons for 'Local', 'Remote', and 'Local & Remote', with 'Local & Remote' selected.
 - PSTN Number**: A text field containing 'NC'.
 - SPID**: A text field containing 'NC'.
- B Channel 2**:
 - Status**: Radio buttons for 'Enable' and 'Disable', with 'Disable' selected.
 - Type**: Radio buttons for 'Local', 'Remote', and 'Local & Remote', with 'Local & Remote' selected.
 - PSTN Number**: A text field containing 'NC'.
 - SPID**: A text field containing 'NC'.

At the bottom of the dialog are five buttons: 'OK', 'Default', 'Send', 'Retrieve', and 'Help'.

Remote Gateway 9150 ISDN BRI Interface information— for Norway and Sweden only

EN 60950:1992 Annex ZB, Special National conditions, Clause 6.2.1.2 states that in Norway and Sweden, supplementary insulation for a primary circuit is required between a Telecommunications Network Voltage (TNV) circuit and any circuit that has a connection to a protective earthing terminal.

The Remote Gateway 9150 unit has the ability to support up to four ISDN BRI circuits. To comply with the specification for supplemental insulation, an isolation adapter must be placed between each of the Remote Gateway 9150 unit BRI inputs and the BRI lines from the service provider.

Isolation adapters are available from local vendors. You can also order the adapters from Nortel as a merchandise item. The Nortel part number is P0935714.

ISDN Line Type

The line type you select determines the options available in the Switch Type list box and the Automatic default coding law (Companding Algorithm) used by the ISDN BRI module being configured. To select a different coding law setting, click on the Coding Law on the 9150 System Configuration property sheet. Refer to “Companding Algorithm” on page 181 for further details.

Choose the ISDN line type according to the following table:

Line Type	Default Coding Law
Proprietary Switch	μ-law
National ISDN – 1	μ-law
National ISDN – 2	μ-law
National ISDN – 3	μ-law
National ISDN – 4	μ-law
Japan NTT	μ-law
France	A-law
Germany	A-law
ETSI EuroISDN	A-law

Line Type	Default Coding Law
United Kingdom	A-law
Australia	A-law
DPNSS 1	μ-law
DASS 2	μ-law

Automatic TEIs (Terminal Endpoint Identifiers)

BRI modules must be used in a point-to-point configuration if using automatic TEI assignments. They cannot be used in a multi-point configuration. Also, make sure that no other ISDN devices are on the line.

Entering the BRI settings

To enter the BRI settings:

- 1 Complete the fields as described in “BRI Configuration field descriptions” on page 228.
- 2 Click on the **OK** button
Result: Configuration Manager writes the changes to a temporary file on the administration PC.
- 3 Click on the **Send** button to update the Remote Gateway 9150 unit with the new information.

Note: To save changes to the Remote Gateway 9150 unit's Flash memory, select Upload → Save to Flash from the Menu Bar.

BRI Configuration field descriptions

Field	Description
Module #	<p>Select the number identifying the trunk interface module that you are configuring.</p> <p>Note: The number you select must match the module position where the module has been installed.</p> <p>Valid options are 4 through 7.</p> <p>The default is four.</p>
TEI Dropped	<p>When the layer 2 drops, the TEI also drops and must be re-acquired.</p> <ul style="list-style-type: none">■ Click on the Enable option button if you want the TEI to drop when the layer 2 drops.■ Click on the Disable option button if you do not want the TEI to drop when the layer 2 drops. <p>The default is Disable.</p> <p>Note: This is a CO implementation dependent configuration.</p>

Field	Description																												
ISDN Line Type	<p>Select the type of ISDN line used in your country. The line type you select determines the options available in the Switch Type drop down list box and the Automatic default coding law (Companding Algorithm) used by the ISDN BRI module being configured. To select a different coding law setting, select the Companding Algorithm on the 9150 System Configuration property sheet. For more information on this setting, refer to “Companding Algorithm” on page 185.</p> <p>Choose the ISDN line type according to the following:</p> <table><tr><th>Line Type</th><th>Default Coding Law</th></tr><tr><td>Proprietary Switch</td><td>μ-law</td></tr><tr><td>National ISDN - 1</td><td>μ-law</td></tr><tr><td>National ISDN - 2</td><td>μ-law</td></tr><tr><td>National ISDN - 3</td><td>μ-law</td></tr><tr><td>National ISDN - 4</td><td>μ-law</td></tr><tr><td>Japan NTT</td><td>μ-law</td></tr><tr><td>France</td><td>A-law</td></tr><tr><td>Germany</td><td>A-law</td></tr><tr><td>ETSI EuroISDN</td><td>A-law</td></tr><tr><td>United Kingdom</td><td>A-law</td></tr><tr><td>Australia</td><td>A-law</td></tr><tr><td>DPNSS</td><td>μ-law</td></tr><tr><td>DASS</td><td>μ-law</td></tr></table> <p>The default is Proprietary Switch.</p>	Line Type	Default Coding Law	Proprietary Switch	μ-law	National ISDN - 1	μ-law	National ISDN - 2	μ-law	National ISDN - 3	μ-law	National ISDN - 4	μ-law	Japan NTT	μ-law	France	A-law	Germany	A-law	ETSI EuroISDN	A-law	United Kingdom	A-law	Australia	A-law	DPNSS	μ-law	DASS	μ-law
Line Type	Default Coding Law																												
Proprietary Switch	μ-law																												
National ISDN - 1	μ-law																												
National ISDN - 2	μ-law																												
National ISDN - 3	μ-law																												
National ISDN - 4	μ-law																												
Japan NTT	μ-law																												
France	A-law																												
Germany	A-law																												
ETSI EuroISDN	A-law																												
United Kingdom	A-law																												
Australia	A-law																												
DPNSS	μ-law																												
DASS	μ-law																												

Field	Description
Switch Type	<p>Select the type of ISDN switch used by your ISDN service provider.</p> <p>Valid options are Unknown, AT&T, Northern Telecom, and Siemens.</p> <p>The default is Unknown.</p> <p>Note: Obtain this information from your ISDN service provider.</p>
Status (B channel 1 and B channel 2)	<ul style="list-style-type: none">■ Click on the Enable option button to activate the ISDN BRI channel.■ Click on the Disable option button to deactivate the ISDN BRI channel. <p>The default is Disable.</p>
Type (B channel 1 and B channel 2)	<p>Click on the type of connection option button—Local, Remote, or Local & Remote.</p> <ul style="list-style-type: none">■ Local: This trunk is used for local PSTN calls only.■ Remote: This trunk creates a PSTN connection path to the host PBX.■ Local & Remote: This trunk can route local PSTN calls and host PBX calls. <p>The default is Local & Remote.</p> <p>Notes:</p> <ol style="list-style-type: none">1. If your Remote Gateway 9150 unit has multiple BRI modules, configure a maximum of one BRI module as Remote Only if PSTN connections are required. Configure all other BRI modules as Local only.2. If your Remote Gateway 9150 unit has just one BRI module, the BRI module can be configured as Local only or Remote only. If local ISDN calls and remote calls over PSTN are required, then MSN must be enabled.

Field	Description
PSTN Number (B channel 1 and B channel 2)	<p>Enter the full telephone number provided to you by your ISDN service provider for this B-channel. Include access codes, dialing prefix, and area code if necessary.</p> <p>When entering the area code, always enter it directly before the main telephone number. Do not use a hyphen (-) as a separator because hyphens are reserved for subaddressing.</p> <p>The default is NC (Not Configured).</p>
SPID (B channel 1 and B channel 2)	<p>Enter the Service Profile Identifier (SPID) provided to you by your ISDN service provider for this B-channel.</p> <p>The default is NC (Not Configured).</p>

Trunk group configuration

This section explains how to enable and create trunk groups for use with the Remote Gateway 9150 unit and how to configure your trunks to either connect with the RLC at the host site or to place calls through the local PSTN. For more information, refer to “Trunk groups” on page 234 and “Trunk access codes” on page 234.

Getting there 9150 → Configuration Manager → Trunk Group Configuration

Trunk Group Configuration property sheet

The screenshot shows a software window titled "TRUNK GROUP CONFIGURATION". Inside, there is a section labeled "Trunk Groups" which contains several controls: a "Group No" dropdown menu set to "1", a "Status" section with radio buttons for "Enable" and "Disable" (where "Disable" is selected), a "Trunk Access Code" text field containing "#61", and a "Local DN's to Alert" section with a checked checkbox labeled "Not Configured" and five empty text input boxes. Below these is a button labeled "Trunk Group B Channels...". At the bottom of the window are five buttons: "OK", "Default", "Send", "Retrieve", and "Help".

Trunks

A trunk is the straight connection between the PSTN and the Remote Gateway 9150 unit. Each ISDN BRI line (up to four are supported by the Remote Gateway 9150 unit) provides two B-channels. In Remote Gateway 9150 unit context, each B-channel equals one trunk.

Each B-channel can be defined as a local trunk, remote trunk, or both.

Note: Remote Gateway 9150 unit support MSN. If each B-channel has a unique DN then the configuration of the first B-channel defines both B-channels. For more information on MSN, refer to “Multiple Subscriber Numbering (MSN)” on page 13.

Local trunk

The trunk is used to place local calls over the PSTN.

Remote trunk

A remote trunk is used to establish a connection to the RLC from the Remote Gateway 9150 unit.

Local and remote trunk

A B-channel that is defined as both local and remote can be used to place calls through both the local PSTN, and the RLC on the host PBX.

Primary trunk on the Remote Gateway 9150 unit

The primary trunk on the Remote Gateway 9150 unit is one of the following:

- the lowest-numbered B-channel defined as Remote only
- the lowest-numbered B-channel defined as Local and Remote

A local call can cause blocking of an incoming host-controlled call on a B-channel defined as Local and Remote, or prevent QoS transitions from occurring. Therefore, Nortel recommends that you configure the primary trunk as Remote only. For example, Module 4 first B channel.

Do not include the primary trunk in any trunk groups.

Trunk groups

A trunk group consists of one or more B-channels that are logically grouped. You can configure up to eight trunk groups. For example, you can configure:

- each B-channel as a different trunk group
- two or more B-channels as a trunk group

A B-channel can be a member of more than one trunk group.

Trunk access codes

Trunk access codes are numbers that are used by the Remote Gateway 9150 unit to determine which trunk group to use when routing the call. You must define a trunk access code for each trunk group.

For example, you can assign trunk access codes #61 and #62, as shown below:

Group 1	Group 2
Trunk 1	Trunk 3
Trunk 2	Trunk 4
Trunk access code: #61	Trunk access code: #62

If a user dials trunk access code #61, the call is routed (or processed) using trunks 1 or 2. If trunks 1 and 2 are both busy, the user’s call is blocked (the user receives a fast busy signal).

Note: All trunk access codes are automatically prefixed in Configuration Manager with a pound sign (#) so that there are no conflicts with host PBX dialing plans. Trunk access codes must be between one and three digits in length in addition to the pound sign.

For a list of the default trunk access codes, refer to the “Remote Gateway 9150 Configuration Information—Dialing Plans on page 384.

ISDN configuration

In order to configure European ISDN, the PSTN must support the following features:

- Multiple Subscriber Numbering (MSN)
- Two directory numbers (one per B channel)

The default configuration setting for BRI SPIDs is NC (Not Configured). Ensure that no supplemental ISDN services, (for example, Call Waiting) are provided as this may disrupt the data path and drop calls.

European ISDN

When configuring EuroISDN and ETSI variants, the BRI Configuration SPIDs must be set to NC (not configured).

To change EuroISDN SPID values, complete the following procedure:

- 1 Go to Configuration Manager > 9150 > BRI Configuration.
- 2 Click on the **Default** button.
- 3 Configure the DNs, SPIDs, and ISDN line type.

Note: Only A-Law configuration is fully supported with ETSI configurations.

National ISDN

If you select National ISDN as the line type, there are minor protocol differences between National ISDN -1, -2, -3, and -4. The Proprietary Switch line type is more general and is an acceptable alternative if you encounter problems.

Configuring trunk groups

To configure trunk groups:

- 1 Complete the fields as described in “Trunk Group Configuration field descriptions” below.
- 2 Click on the **OK** button
- 3 Click on the **Send** button to update the Remote Gateway 9150 unit with the new information.

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

Note: To save changes to the Remote Gateway 9150 unit's Flash memory, select Upload → Save to Flash from the Menu Bar.

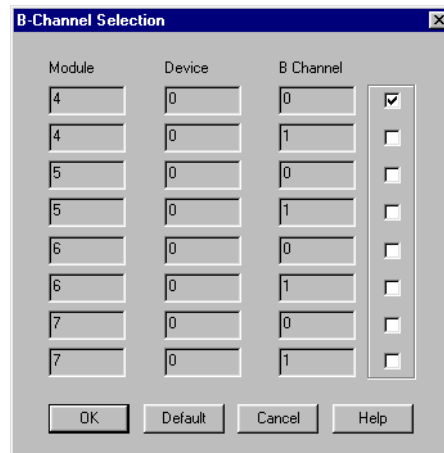
Trunk Group Configuration field descriptions

Field	Description
Group No	<p>Select a group number.</p> <p>Valid options are 1 through 8.</p> <p>The default is 1.</p>
Status	<ul style="list-style-type: none">■ Click on the Enable option button to activate the trunk group.■ Click on the Disable option button to deactivate the trunk group. <p>The default is Disable.</p>
Trunk Access Code	<p>Enter the trunk access code that you want to assign to the trunk group, or accept the default.</p> <p>Note: The trunk access code is automatically prefixed with a pound sign (#). This means users must dial the # before the trunk access code when making an outgoing local call.</p> <p>Maximum length: 1 to 3 digits in addition to the pound sign</p> <p>The default is 61.</p>
Local DNs to Alert: Not Configured	<p>Ensure that the Not Configured check box is cleared if you wish to have incoming calls ring only on specific stations. Enter the applicable extensions in the fields below the check box. You can enter up to five extensions.</p> <p>Note: You can create a private line by dedicating a trunk group to one station only.</p> <p>If you leave the fields blank, incoming calls received by this trunk group rings on all telephones.</p>

Field**Description****Trunk Group
B Channels**

Click on the **Trunk Group B Channels** button.

Result: The Trunk Group B-Channel dialog box displays.



The B-Channel Selection dialog box contains a table with three columns: Module, Device, and B Channel. There are eight rows of input fields. To the right of the B Channel column is a column of checkboxes. At the bottom are four buttons: OK, Default, Cancel, and Help.

Module	Device	B Channel	
4	0	0	<input checked="" type="checkbox"/>
4	0	1	<input type="checkbox"/>
5	0	0	<input type="checkbox"/>
5	0	1	<input type="checkbox"/>
6	0	0	<input type="checkbox"/>
6	0	1	<input type="checkbox"/>
7	0	0	<input type="checkbox"/>
7	0	1	<input type="checkbox"/>

Buttons: OK, Default, Cancel, Help

Complete the fields as follows:

- **Module:** This field displays trunk interface module numbers.
- **Device:** This field displays the internal device number for each B-channel provided by the module.
- **B Channel:** This field displays B-channel numbers.
- **Check boxes:** Click on the check box for each B-channel you want to be part of this trunk group.

Note: A B-channel can be a member of more than one trunk group.

Click on the **OK** button.

DSP configuration

This section shows you how to configure DSP resources on your Remote Gateway 9150 unit. The Remote Gateway 9150 unit must provide the same number of voice DSP channels as the maximum number of simultaneous calls your remote services network supports. Each DSP *module* holds two DSP *devices*. Currently, each DSP *device* holds four DSP *channels*. To add eight DSP *channels* to your Remote Gateway 9100 Series system's voice processing capability, add one DSP application *module*.

Getting there 9150 → Configuration Manager → DSP Configuration

DSP Configuration property sheet

DSP CONFIGURATION

Module Number: 0

No of Devices: 2

Device Number 1

DSP Load: AUTO

Compression Algorithms: G.729A, G.726, G.711

Device Number 2

DSP Load: AUTO

Compression Algorithms: G.729A, G.726, G.711

OK Default Send Retrieve Help

Module identification

The upper portion of the DSP configuration property sheet displays fields that identify the module you are currently configuring. In the Module Number drop down box, choose the module position on the Remote Gateway 9150 unit that the DSP module occupies. Module 0 represents the built-in DSP resources on the Remote Gateway 9150 unit—the equivalent of one DSP application module.

Device configuration

The middle portion of the property sheet displays information describing the DSP loads, and corresponding compression algorithms that you can select for each DSP device.

Configuring DSPs

To configure DSPs on your Remote Gateway 9150 unit, complete the following steps:

- 1 Access the DSP Configuration property sheet.
- 2 Complete the fields as described in “DSP Configuration field descriptions” on page 241.
- 3 Click on the **OK** button
Result: Configuration Manager writes the changes to a temporary file on the administration PC.
- 4 Click on the **Send** button to update the Remote Gateway 9150 unit with the new information.

Note: To save changes to the Remote Gateway 9150 unit’s Flash memory, select Upload → Save to Flash from the Menu Bar.

DSP Configuration field descriptions

Field	Description
Module Number	<p>Select the number of the module that the DSP devices that you want to choose compression algorithms for are located on.</p> <p>Note: Module 0 represents the main board (RLC or Remote Gateway 9150 unit). Modules 1 and higher represent plug-in modules.</p> <p>The default is 0.</p>
No of Devices	<p>This is a read-only window displaying the number of DSP devices on the DSP module you selected in the Module Number field. Refer to “Configuring DSPs” on page 240 for an explanation of DSP <i>devices</i> versus DSP <i>modules</i> and DSP <i>channels</i>.</p> <p>Device Number 1 or 2</p>
DSP Load	<p>Select the DSP Load providing the collection of compression algorithms that you would like loaded on the selected DSP according to the compression algorithms displayed in the Compression Algorithms window.</p> <p>Valid options are G.729A, 911X, G.723_CONF, and AUTO.</p> <p>The default is AUTO.</p> <p>Notes:</p> <ol style="list-style-type: none">1. G.723_CONF allows you to record telephone calls using IDVR. For more information regarding IDVR, contact your TelStrat representative.2. Selecting AUTO instructs the Remote Gateway 9150 unit to choose a default DSP load. This default load is G.729A, depending on DSP channel availability.

Field	Description
Compression Algorithms Note: This description applies to both appearances of this field.	<p>This read-only window displays the combination of compression algorithms that are available in the DSP load selected in the DSP Load drop down list.</p> <p>The compression algorithm (G.711, G.726, or G.729A) used on calls to or from the Remote Gateway 9100 Series unit stations is dictated by the compression setting configured for the remote port that the call is processed over.</p>

Auto upgrade configuration

Use the Auto Upgrade Configuration property sheet to automatically or on a scheduled basis query a predefined TFTP server and upgrade the firmware for Remote Gateway 9100 Series units.

Getting there RLC → Configuration Manager → Auto Upgrade Configuration

Auto Upgrade Configuration property sheet

The screenshot shows a window titled "AUTO UPGRADE CONFIGURATION". Inside, there is a "Status" section with two radio buttons: "Enable" and "Disable", with "Disable" selected. Below this is a "TFTP Server" section with an "IP Address" field consisting of four boxes, each containing a "0". To the right of the IP address field is a "Start Auto Upgrade" button. Below the TFTP Server section is a "Frequency" section with three radio buttons: "Once a Day", "Once a Week", and "Once a Month", with "Once a Day" selected. Below the Frequency section are three fields: "Time" set to "00:00", "Day" set to "Sunday" (with a dropdown arrow), and "Date" set to "1". At the bottom of the window are five buttons: "OK", "Default", "Send", "Retrieve", and "Help".

Configuring automatic upgrade

To configure automatic upgrade of your Remote Gateway 9150 unit, complete the following steps:

- 1 Access the Auto Upgrade Configuration property sheet.
- 2 Complete the fields as described in “Auto Upgrade Configuration field descriptions” on page 245.
- 3 Click on the **OK** button.

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

- 4 Click on the **Send** button to update the Remote Gateway 9150 unit with the new information.

Note: To save changes to the Remote Gateway 9150 unit's Flash memory, select Upload → Save to Flash from the Menu Bar.

Auto Upgrade Configuration field descriptions

Field	Description
Status	<ul style="list-style-type: none">■ Click on the Enable option button if you want to automatically or on a scheduled basis query a predefined TFTP server and upgrade the firmware for Remote Gateway 9100 Series units.■ Click on the Disable option button if you do not want to automatically or on a scheduled basis upgrade the firmware for Remote Gateway 9100 Series units. <p>The default is Disable.</p>
TFTP Server: IP Address	Enter the IP address of the TFTP server you want to query for the upgrade.
Start Auto Upgrade	<p>Click on the Start Auto Upgrade button to force the auto upgrade process to begin regardless of the mode and time configuration in the auto upgrade configuration.</p> <p>Note: Use caution when forcing the auto upgrade process as the system performs a self-reset on all units to make the new firmware active once the download of new firmware is complete.</p>
Frequency	<p>Click on the option button that identifies how often you want the unit to perform the auto upgrade process:</p> <ul style="list-style-type: none">■ Once a Day■ Once a Week■ Once a Month
Time	Select the time of day that you want the unit to perform the auto upgrade process.
Day	Select the day when you want the auto upgrade process to be performed (if you selected "Once a Week" in the Frequency field).

Field	Description
Date	Select the date when you want the auto upgrade process to be performed (if you selected "Once a Month" in the Frequency field).

Syslog configuration

Use the Syslog Configuration property sheet to enable syslog functionality and configure up to three syslog server IP addresses for logging all events (display logs) to the syslog server(s) you configure. This feature allows event logs (display logs) to be retained if you reboot or restart the Remote Gateway 9100 Series unit. Remote Gateway 9100 Series supports the following syslog collector software:

- Kiwi Syslog Daemon - www.kiwisyslog.com
- WinSyslog - www.winsyslog.com
- tftpd32 server - <http://tftpd32.jounin.net>

Getting there 9150 → Configuration Manager → Syslog Configuration

Syslog Configuration property sheet

SYSLOG CONFIGURATION

Status

☒ Enable
☐ Disable

IP Address 242 . 158 . 15 . 15 →

Syslog Servers (max. 3):

Delete

Facility Indicator Local Use 0

OK Default Send Retrieve Help

Configuring syslog functionality

To configure syslog functionality on your RLC, complete the following steps:

- 1 Access the Syslog Configuration property sheet.
- 2 Complete the fields as described in “Syslog Configuration field descriptions” on page 249.
- 3 Click on the **OK** button.

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

- 4 Click on the **Send** button to update the RLC with the new information.

Note: To save changes to the RLC's Flash memory, select Upload → Save to Flash from the Menu Bar.

Syslog Configuration field descriptions

Field	Description
Status	<ul style="list-style-type: none">■ Click on the Enable option button if you want to enable the syslog functionality.■ Click on the Disable option button if you do not want to enable the syslog functionality. <p>The default is Disable.</p>
IP Address	<p>Enter the IP Address of the syslog server. Then, press the Enter key or click on the -> button to add the IP address to the Syslog Servers window. You can enter up to three syslog server IP addresses.</p> <p>Result: The IP address of the syslog server displays in the Syslog Servers window.</p>
Delete	<p>To delete a syslog server IP address from the Syslog Servers window, click on the specific IP address that you want to delete and then click on the Delete button.</p>
Facility Indicator	<p>Select the facility indicator from the drop down box.</p> <p>Valid options are Local Use 0 through 7.</p>

Station configuration

This section explains how to configure the Remote Gateway 9150 unit so that it can:

- route calls between the stations at your site and the host PBX
Each station is associated with a port on the RLC, and can be configured with different capabilities.
- place calls through the local PSTN or to other stations at the Remote Gateway 9150 site

If resources on the RLC on the host PBX allow, you can configure up to 32 telephone stations plus one analog device (such as an analog telephone or fax machine). This configuration assumes that none of the stations are equipped with Analog Telephone Adapters (ATAs) or Meridian Communication Adapters (MCAs).

Bridge Ports

Bridge Ports are proxy ports that represent local calls or inbound PSTN calls to the PBX. When a local call on a Remote Gateway 9150 unit needs PBX services, the Bridge Port obtains a PBX presence on behalf of the local call.

When configuring Bridge Ports:

- Consider the number of simultaneous remote service telephone calls and the number of bridge ports in use when determining PSTN or IP bandwidth needs.
- Remember that every local ISDN call reduces the PSTN bandwidth available for remote service telephone calls and bridge ports when determining needed PSTN bandwidth.

Notes: You can configure a maximum of sixteen (16) Bridge Ports. You must configure at least one SCR key on the set for the Bridge Port feature to work.

You must configure Bridge Port parameters on both the host PBX and the Remote Gateway 9150 unit. For every Bridge Port defined on the Remote Gateway 9150 unit you must configure an SCR key with voice capability on key 0 for that port on the host PBX. For more information on configuring SCR keys on a host PBX refer to your PBX documentation.

Note: Local Only digital telephone sets do not support conference calls to a local Remote Gateway 9150 unit or to a host PBX. Local Only digital telephone sets can dial host PBX DN's using an enabled Bridge Port.

Configuring Bridge Ports reduces the total number of ports available from the RLC.

Call processing capabilities and station settings

Each station can be defined as a telephone that can process:

- local calls only
- remote calls only
- local and remote calls

Stations defined with local call capability are further defined with telephone features and local call appearance keys. Stations that are defined with remote call capability do not need to be further configured because they inherit their features and call appearance keys from their associated port configurations on the host PBX.

Local call capability

Stations defined as *local* can place and receive calls through the local PSTN or to other stations at the Remote Gateway 9150 site. Calls through the host PBX are not allowed.

Local stations are not associated with RLC ports.

Remote call capability

Stations defined as *remote* are associated with RLC ports, and can place and receive calls through the host PBX only. Calls through the local PSTN are not allowed.

Local and remote call capability

Stations defined as *Local and Remote* are associated with RLC ports, and can

- place and receive calls through both the host PBX and the local PSTN
- place calls to other stations at the Remote Gateway 9150 site

Outgoing calls are routed according to the call appearance key used to initiate the call.

- Calls initiated on the key defined as the host call appearance key (also referred to as the *primary DN key*) are routed through the host PBX.
- External calls initiated on the key defined as the local call appearance key are routed through the local PSTN.
- Internal calls initiated on the local call appearance key are routed to other stations at the Remote Gateway 9150 site.

The Remote Gateway 9150 unit distinguishes an incoming call by its calling line identification, and rings it as follows:

- on the host call appearance key if the call was routed through the host PBX
- on the local call appearance key if the call was routed through the local PSTN or if the call was a station-to-station call

Local station settings

When a station is defined with local capability, you can further configure the station to:

- enable or disable certain features (for more details, refer to “9150 port configuration” on page 207)
- disable outgoing dialing digit sequences (refer to “Disabled Outbound Digit Sequence” on page 212)
- identify local call appearance and feature key positions (refer to “Optional Feature Keys” on page 213)

Remote station settings

When the station is defined with remote capability, you can assign it to a specific port on the RLC (refer to “9150 port configuration” on page 207).

Call appearance keys

The host call appearance key is defined for each station on the host PBX. It is not defined for each station on the Remote Gateway 9150 unit.

The local call appearance keys, on the other hand, must be defined for each station connected to the Remote Gateway 9150 unit to allow:

- users to place outgoing calls using Remote Gateway 9150 trunks
- users to place station-to-station calls without host PBX control
- incoming calls on Remote Gateway 9150 trunks to ring specific stations

The local call appearance keys must be left undefined in the host PBX configuration to avoid indicator conflicts between the host PBX and the Remote Gateway 9150 unit. Only indicators defined as local call appearances are blocked from the host PBX.

Any active Single Call Ringing (SCR)/Single Call No-ringing (SCN) key causes the Remote Gateway 9100 Series unit to allocate DSP and WAN bandwidth for that port. This supports a privacy over-ride feature available with the SCR/SCN key. To avoid using unnecessary bandwidth, Nortel recommends that you use Multiple Call Ringing (MCR)/Multiple Call No-ringing (MCN) keys for Multiple Appearance Directory Number (MADN) appearances at remote sites.

When to configure the local call appearance keys

The local call appearance key positions must be defined when a new station is being configured with local capability, or when a request to change feature key positions has been initiated.

Dial tone delay

Telephone sets connected to Remote Gateway 9150 units can experience unexpectedly long dial tone delay. Specific delays depend on the number of associated MADN appearances and the system activity at the time the call is attempted. If you configure more than five to six MADNs on a single Remote Gateway 9100 Series system, the signaling can become delayed and result in sporadic ringing.

Note: This applies to all SCR, SCN, MCR, and MCN keys.

When placing a telephone call, the dial tone is delayed from the time that the user goes off-hook. The duration of this delay depends on the number of simultaneous calls actually being set up. With Remote Gateway 9100 Series, the dial tone delay is equal to the number of appearances, or calls, multiplied by approximately 300 milliseconds (ms), or 0.30 seconds (s).

Therefore, when placing a call from a Remote Gateway 9100 Series MADN with 10 appearances, expect a dial tone delay of approximately 3000 ms, or 3 s:

$$10 \text{ appearances} \times 300 \text{ ms} = 3000 \text{ ms}$$

The following table calculates approximate Remote Gateway 9100 Series dial tone delay for three different scenarios:

Number of appearances	Call set-up duration	Remote Gateway 9100 Series dial tone delay
1	300 ms (0.30 s)	300 ms (0.30 s)
5	"	1500 ms (1.50 s)
10	"	3000 ms (3.00 s)

Note: If you start from an idle state, include time for ISDN line set-up, which can be as much as an additional 4–6 seconds.

Associating trunk groups with local stations

Each trunk group can be defined to ring only specific stations. This feature allows you to route certain types of calls (such as incoming calls on a 1-800 number) to specific stations.

MCR keys increase DSP requirements

In determining the DSP requirements of your Remote Gateway 9100 Series system, your calculations must consider the number of ports containing MCR keys. The over-riding concept to keep in mind when determining DSP requirements is that each ringing or answered telephone call requires one DSP channel.

The following example assumes one 16-port RLC with no additional DSP Application Modules, for an RLC with eight DSP channels.

Example: While one telephone call is active, which uses one DSP channel, a call to an MCR key assigned to eight Terminal Numbers (TNs) produces a DSP allocation error. The seven available DSP channels are insufficient for this call. A non-blocking configuration must include one DSP channel for each simultaneously ringing or active digital telephone set that you want to support.

Private lines

A private line is a telephone line that is used by one person only. Calls that are routed to the private line do not ring on any other station in your office. To dedicate a private line to a station, configure a trunk group to ring incoming calls only on that station.

If you are connecting a fax machine to the Remote Gateway 9150 unit, then configure a private line to the fax. Incoming calls on this line are routed directly to the fax.

For instructions, refer to “Trunk group configuration” on page 232.

Calling permissions and restrictions

You can consider the ability to place certain types of calls from a station to be a calling permission. Similarly, a certain type of call that is not allowed is a calling restriction.

You can define both permissions and restrictions for each station.

Local and remote calling permissions

When you define a station as a local station, you are granting the station with local calling permission. Calls can be made or received through the local PSTN or to and from other stations. Calls through the host PBX are not allowed.

When you define a station as a remote station, you are granting the station with remote calling permission. Calls can be made or received through the host PBX only. Calls through the local PSTN are not allowed.

Exception: If the emergency service number is configured on the Remote Gateway 9150 unit and you are using the PSTN to route calls, the dialed emergency service number is routed through the local PSTN to the emergency service. This ensures that the emergency service receives the correct calling location information.

When you define a station as a local and remote station, you are granting the station with the ability to place or receive calls through both the local PSTN and the host PBX. Station-to-station calls are also allowed.

Call restriction

You can prevent certain types of calls from being made at a station by disabling the digits that normally allow the call to proceed. This option is available for stations designated as Local or both Local and Remote.

For example, if you want to prevent someone from calling a 1-976 number, enter 1976 as the digits to disable. For more information refer to “Disabled Outbound Digit Sequence” on page 212, in the Local Profile Configuration field description section.

ATA- and MCA-equipped stations and bandwidth requirements

Each station equipped with an MCA requires a full 64 Kbps of bandwidth to the host PBX.

For stations equipped with ATA devices, the bandwidth used by calls processed on those stations is as follows:

IF using	THEN
G.729A compression and the call is a voice call,	the voice call is sent as 8 Kbps to the host PBX.
G.729A/Fax compression and the call is a fax call,	the fax call is sent as 9600 bps.
G.711 compression (uncompressed) and the call is a fax call	the fax call is sent as 64 Kbps.
the call is a local call,	the voice call is not compressed. It is sent as 64 Kbps of data across the ISDN BRI B-channel.

The following table identifies the number of MCAs or ATAs that can be connected to the Remote Gateway 9150 unit:

IF the Remote Gateway 9150 unit is connected to	THEN you can connect
a 1-slot RLC (supporting 16 users),	four MCAs or ATAs to the Remote Gateway 9150 unit.
a 2-slot RLC (supporting 32 users),	seven MCAs or ATAs to the Remote Gateway 9150 unit.

Notes:

- You can have eight MCAs or ATAs installed if an analog telephone or fax machine is *not* installed.
- You can have up to 32 digital telephone sets, one fax machine, and seven ATA/MCAs installed. However, only 32 simultaneous calls can be made.

Chapter 6

Using Remote Gateway 9150 stations

In this chapter

Modes of operation	260
Placing and receiving calls	264
Indicator updates	268
Display messages	270
Telephone features operation	273
Going online and offline	277

Modes of operation

Digital telephones at your Remote Gateway 9150 site can operate in the following modes:

- host-controlled
- locally controlled
- online to host PBX
- offline from host PBX

Host-controlled mode

Host-controlled mode means that the host PBX controls the following:

- some display messages that display on your telephone
- indicator updates such as the message waiting indicator
- calls that you receive from or place to someone at the host PBX site

In host-controlled mode, a voice path is established to the host PBX and signaling messages are passed between the host PBX and the Remote Gateway 9150 unit.

Exception: If Local Switchover is enabled, and the station-to-station call is completed through the host PBX, signaling messages are passed between the host PBX and Remote Gateway 9150 unit normally. However, the voice path is established by the Remote Gateway 9150 unit without consuming host connection bandwidth. The host PBX is aware that the call is active and tracks the status of the telephone set.

If the call cannot be completed through the host PBX, you hear a reorder dial tone.

Locally controlled mode

Locally controlled mode means that the Remote Gateway 9150 unit at your site controls the following:

- calls to other stations at this site
- calls that are made to or received from your community through your local telephone service provider

Local calling at the Remote Gateway 9150 unit always results in a call's being placed to the first port with the dialed number. Remote Gateway 9100 Series does not support multiple DN appearances for local calling on the Remote Gateway 9150 unit. Therefore, you cannot configure the same DN to local calling keys on multiple digital telephone sets connected to one Remote Gateway 9150 unit.

Refer to “DN Discovery” in the Reach Line Card Installation and Administration Guide (NTP 555-8421-210) for further details.

In addition, local trunk numbers cannot be pre-dialed. You must wait for the local trunk dial tone before dialing the number.

Relationship between host-controlled and locally controlled modes

Both the host-controlled and locally controlled modes can be used at the same time. When placing or receiving calls, the call modes are controlled by the following telephone keys:

- the host call appearance key (also known as the *primary DN* key)
- the local call appearance key (can sometimes be referred to as the *secondary DN* key)

Host call appearance key

The host call appearance key is the main key you use to place and receive calls. For example, if someone from Finance at Head Office calls you, the call rings on this key. Similarly, if you need to call someone in Payroll at Head Office, you place the call on this key.

Local call appearance key

The local call appearance key is the key you use to place and receive local calls. For example, if your office is working overtime and everyone wants pizza, you call the pizza delivery place on the local call appearance key. Similarly, you use this key if you want to call one of your customers or suppliers or someone else at your site.

Your telephone can have up to two local call appearance keys. Your system administrator can tell you where these keys are and how they are labeled.

Online mode

When in online mode, calls initiated on the host call appearance key are directed through the host PBX. Any long distance charges associated with calls placed through the PBX over the PSTN are charged to the host PBX site. The display on all digital telephones shows “Online Mode.”

Offline mode

When in offline mode, you cannot place calls through the host PBX over either the IP network or PSTN. You can only place calls through your local telephone service provider if your station has been granted locally controlled call capability. The display on all digital telephones show “Offline Mode.”

Why offline mode is important

Your organization is concerned about telephone costs and, as such, wants to ensure that the ISDN BRI line at your site is used for host-controlled calls during business hours only. This is especially important when the ISDN BRI connection between the host PBX and your site is defined as *permanent* (always on) rather than *on demand*. A permanent ISDN BRI connection means the line remains active all the time and incurs charges unless it is put into offline mode.

What controls the online and offline modes

The online and offline modes can be controlled by one or both of the following:

- the online/offline schedule configured for your site on the RLC at the host PBX
- special prefix (SPRE) codes configured on the Remote Gateway 9150 unit at your site

Online/offline schedule at host PBX

If telephone service costs are an issue, your telecom network administrator defines an online/offline schedule on the RLC port assigned to your site. The times that your site is scheduled to be put into online or offline mode are processed by the host PBX.

For example, if your normal business day is from 9:00 a.m. to 5:00 p.m. from Monday to Friday, the schedule for your site instructs the host PBX to put all stations at your site into online mode during those times. For all other time periods, all stations are in offline mode and, therefore, disconnected from the host PBX.

Note: If you initiate a call on a host call appearance key on any station, then full functionality is allowed even if the time period is outside the automatic offline periods defined on the RLC.

SPRE codes used at your site

If SPRE codes have been defined on the Remote Gateway 9150 unit at your site, your site can control the times that stations are put into online or offline modes. You do this by entering one of the following codes on any digital telephone at your site:

- Online SPRE code
- Offline SPRE code

It is recommended that one person at your site be designated as the person responsible for putting the Remote Gateway 9150 unit (and all stations) into online mode at the beginning of the business day, and into offline mode at the end of the day.

For information about going online or offline, refer to “Going online and offline”, on page 277.

Placing and receiving calls

The way that you place outgoing calls depends on the call appearance key you use to place the call.

The call appearance key used to receive calls depends on the source of the call.

Receiving incoming calls

The calling line identification (CLID) of an incoming call determines which call appearance key accepts the call.

IF the call	THEN the call
information contains a Called Party Number Display (CPND) that matches a telephone number assigned to one of the ISDN BRI B-channels from your telephone service provider,	<p>is routed to the station based on the DNs to Alert configuration on the trunk group that includes the B-channel. If the DNs to Alert fields are blank, the call rings on all stations.</p> <p>The call rings on the first local call appearance key on all stations that have been designated to receive calls from this trunk.</p> <p>Note: If the first call appearance key is already busy with a call, the call is presented on the second call appearance as a call waiting. The indicator flashes and an alert tone sounds.</p>
comes in on the communication path between the RLC and Remote Gateway 9150 unit,	<p>is routed to the station based on the Remote Gateway 9150 station to RLC port assignment in the Remote Gateway 9150 unit's ports configuration.</p> <p>The call rings on the host call appearance key.</p>
information contains the DN of another station at this site,	rings on the local call appearance key.

Methods for placing outgoing calls

You can place an outbound call from a Remote Gateway 9150 station in one of the following ways:

- Method 1: Pick up the handset.

This method automatically initiates a host-controlled call.

Note: If you then press the local call appearance key, the dial tone from the host PBX is changed to locally controlled mode, and the host PBX connection is released.

- Method 2: Press a call appearance key.

When you press the host call appearance key, a host-controlled call is initiated. When you press the local call appearance key, a locally controlled call is initiated.

Placing host-controlled calls

To place host-controlled calls:

- 1 Pick up the handset or press the host call appearance key.

Result: A connection is established with the host PBX and you hear dial tone.

Note: If a connection to the host PBX cannot be established within a time-out period or no resources are available to carry the call, you hear a re-order dial tone (a fast busy signal), and the following message displays on the telephone display:

Release and Try Again

- 2 Dial the number of the party you want to call.

Result: The host PBX receives and processes the dialed digits and rings the called party.

Placing outgoing locally controlled calls

To place outgoing locally controlled calls:

Note: You cannot use this procedure to place calls to the host PBX site. If you try, you hear a reorder dial tone (a fast busy signal) and the following message displays on your telephone display:

Release and Try Again

- 1 Do one of the following:

IF you are using	THEN
an analog or ATA-equipped station,	do the following: <ol style="list-style-type: none">a Pick up the handset. Result: A connection is established with the host PBX and you hear a dial tone.b Dial the Local Calling SPRE code. Result: The connection is switched to the Remote Gateway 9150 unit and you hear a dial tone.
a digital telephone,	pick up the handset, and then press a local call appearance key. Result: A connection is established with the Remote Gateway 9150 unit and you hear a dial tone.

- 2 Dial a trunk access code, if required.

Result: The Remote Gateway 9150 unit obtains a free trunk and you hear another dial tone.

Note: If a trunk is not available, you hear a reorder dial tone (a fast busy signal) and the following message displays on the telephone display:

Release and Try Again

- 3 Dial the number of the party you want to call.

Result: Your local telephone service provider receives and processes the dialed digits and rings the called party.

Calling another station at your site

To call another station at your site:

Place station-to-station calls through the host PBX. This allows all stations configured as multiple appearance DNs (MADNs) to ring and provide access to voice mail if the call is not answered.

If a connection cannot be established through the host PBX, then you can use the local call appearance key to place the station-to-station call.

- 1 Pick up the handset or press the host call appearance key.

Result: A connection is established with the Remote Gateway 9150 unit and you hear a dial tone. The indicator beside the host call appearance key lights.

- 2 Dial the extension of the party you want to call.

Result: The host PBX receives and processes the dialed digits, and rings the station as well as any other stations that include the dialed DN as an MADN appearance.

Note: The MADN stations could be located at another site (such as the host PBX site).

IF the call is answered by	THEN
an MADN station at another site,	a voice path to the host PBX is established and the call proceeds.
a station at this site,	all signaling continues to be processed by the host PBX. However, the actual voice path is connected between the two stations and the Remote Gateway 9150 unit. No trunk bandwidth back to the host PBX is used for the voice path. Trunk bandwidth previously reserved for the call is released and made available to other calls.

Indicator updates

Digital telephone indicators reflect the current status of the telephone. For example, they identify when calls are waiting, active, or on hold, or, if your office has voice mail, that messages have been received.

Indicators are updated as follows:

- by the host PBX when a connection between the host PBX and Remote Gateway 9150 unit is active
- by the Remote Gateway 9150 unit for feature keys defined on stations with local call capability

Host-controlled indicator updates

Indicators for host-controlled features are updated automatically by the host PBX each time:

- an incoming call is received by your site from the host PBX
- an outgoing call is made from your site through the host PBX
- a message waiting indicator (MWI) update is received by someone at your site

Note: If the PSTN is being used and the Remote Gateway 9150 unit is configured with a permanent (always on) connection to the host PBX, the ISDN BRI service is active and telephone indicators are always updated.

If the IP network is being used to route calls, indicators are always updated.

Locally controlled indicator updates

The following indicators are updated by the Remote Gateway 9150 unit (that is, these indicator updates are locally controlled):

- host and local call appearance key indicators

The indicator lights when the handset is taken off-hook, or when you press the call appearance key to go off-hook.

Note: The Remote Gateway 9150 unit passes key presses and the on- or off-hook status for the host call appearance key to the host PBX.

- Handsfree
- Mute

Display messages

This section describes the messages that can display on your digital telephone.

Message descriptions

Message	Description
Going Offline in 30 Secs	This message warns you that all digital telephones at this site are about to go offline in the number of seconds indicated.
Going Offline in 20 Secs	If any calls are active, they are disconnected when the offline mode is activated.
Going Offline in 10 Secs	To override, enter the Online SPRE code.
Hostless Mode	<p>The connection to the host PBX cannot be established. The host PBX might be temporarily unavailable.</p> <p>You can still place local calls by using one of the local call appearance keys.</p> <p>Note: If Hostless Mode persists, contact your system administrator.</p>
Logged In	<p>If this message displays on your station, then your station is associated with a multi-user or dynamic pool port on the RLC, and it is in logged on status.</p> <p>Note: This message displays for approximately ten seconds.</p>

Message	Description
Offline Mode	<p>You cannot place calls through the host PBX over either the IP network or the PSTN.</p> <p>Note: If you need to place a call through the host PBX while in offline mode, press the host call appearance key. This establishes a connection to the host PBX and puts all digital telephones at your site into online mode.</p>
Online Mode	<p>You can place and receive calls through the host PBX.</p>
Port Already in Use	<p>If this message displays on your station, then your station is associated with a multi-user or dynamic pool port on the RLC.</p> <p>This message displays if the port that you are attempting to use is already being used by someone else.</p>
Port Not Logged In	<p>If this message displays on your station, then your station is associated with a multi-user or dynamic pool port on the RLC, but it is in logged off status.</p>
QoS Recovery	<p>The Quality of Service (QoS) has returned to normal on the IP network and your active call is being automatically moved to the IP network.</p>
QoS Transition	<p>The QoS has degraded on the IP network and your active call is being automatically moved to the PSTN.</p>

Message	Description
Release and Try Again	<p>All Remote Gateway 9150 trunks are busy or there are not enough DSP resources to process the call. Try again at a later time.</p> <p>Note: Ensure the call you are placing is initiated from the appropriate call appearance key:</p> <ul style="list-style-type: none">■ host call appearance key: to call someone at the host PBX site■ local call appearance key: to place a local PSTN call or to call another station at your site
Bandwidth Limit	<p>If this message displays on your station and you hear a fast busy signal when you attempt to place a call, then there is insufficient PSTN bandwidth.</p> <p>Wait a moment, and then try your call again.</p>
DSP Limit	<p>If you see this message and hear a fast busy signal when you attempt to place a call, then Digital Signal Processor (DSP) resources are all busy.</p> <p>Wait a moment, and then try your call again.</p>
Call Failure	<p>If you see this message and hear a fast busy signal when you attempt to place a call, then the Remote Gateway 9150 unit failed to establish the PSTN connection to the RLC.</p> <p>Wait a moment, and then try your call again.</p>

Telephone features operation

This section describes how to use the following digital telephone features in host- or locally controlled modes:

- emergency service calls
- Hold
- Call Waiting
- Call Transfer
- Conference
- Call Forward
- Paging

Note: The Conference and Call Forward features are supported for host-controlled calls only.

Emergency service calls

The Remote Gateway 9150 unit allows an emergency number (for example, 911 in North America) to be programmed by your system administrator.

If the PSTN is used to route calls, and someone dials this emergency service number on any station that is connected to the Remote Gateway 9150 unit, the call is processed by your local telephone service provider.

You can initiate the emergency service call on either the host call appearance (primary DN) key or local call appearance key. You do not have to dial a trunk access code first.

ATTENTION!

If only the IP network is being used to route calls, you must use a telephone that is directly connected to the PSTN to place an emergency service call. If you place the call on a station that is connected to the Remote Gateway 9150 unit, the call is routed through the host PBX, which can in a different city.

Hold

How Hold works in host-controlled mode

When you press Hold on a host-controlled call, the holding party receives the Hold treatment defined on the host PBX. For example, if the host PBX is configured to play music to holding parties, then the holding party hears music.

You can press any available call appearance key to place a new call.

How Hold works in locally controlled mode

Normally, you put a call on hold by pressing Hold. However, you can also put a locally controlled call automatically on hold by pressing the other local call appearance key. To use this feature, Auto Hold must be enabled on your station.

If Auto Hold is not enabled, and you press a local call appearance key while a call is active on the other local call appearance key, that call is disconnected.

When you press Hold on a locally controlled call, the holding party hears silence. You can press any available call appearance key to place a new call.

Call Waiting

Since the Remote Gateway 9150 unit does not use host-controlled indicators and the locally controlled indicators are not defined on the host PBX, there are never any indicator conflicts when a call is presented to the station.

However, since the host PBX is not aware when locally controlled calls are active, the host PBX might try to present a call and ring your station while you are busy with a locally controlled call. The Remote Gateway 9150 unit always checks the status of your station before ringing it. If your station is busy with a call, the alert tone is sounded instead.

How Call Waiting works in host-controlled mode

If you are busy with a host-controlled call, incoming calls are handled as follows:

- An incoming host-controlled call is directed to the call waiting key by the host PBX.
- An incoming locally controlled call flashes the local call appearance key indicator and sounds the alert tone.

How Call Waiting works in locally controlled mode

If you are busy with a locally controlled call, incoming calls are handled as follows:

- An incoming host-controlled call flashes the host call appearance key and sounds the alert tone.
- An incoming locally controlled or station-to-station call flashes the next available local call appearance key and sounds the alert tone. If both local call appearance keys are busy, then the call is not presented to your station.

Call Transfer

Call transfer works the same way in both host- and locally controlled modes. The only difference is the treatment the holding party receives, depending on whether the original call is a host-controlled or locally controlled call.

A call on the host call appearance key can be transferred:

- to another station that has remote call capability at this site
- to a station at the host PBX site

A call on the local call appearance key can only be transferred to another station at this site. You cannot transfer a call on the local call appearance key to a station at the host PBX site.

For both, you can do an announced or unannounced (blind) transfer.

Transferring a call

To transfer a call:

- 1 Press the Transfer key.

Result: The active call is placed on hold and you hear a dial tone.

- 2 Dial the number that you want to receive the transferred call.

- 3 Press the Transfer key again to complete the transfer.

Note: You can press the Transfer key while the call is still ringing, or after the called party answers.

When you transfer a local call using the Trunk Access code to dial an outbound local call, the corresponding voice path is not established. Remote Gateway 9100 Series does not support this function.

Conference

The Conference feature is supported for host-controlled calls only. You cannot conference in someone who must be called through the local PSTN.

Placing a conference call

To place a conference call:

- 1 Press the Conference key.
Result: The active call is placed on hold and you hear a dial tone.
- 2 Dial the number of the party you want to conference in.
- 3 When the called party answers, press the Conference key again to complete the conference.

Call Forward

Remote Gateway 9100 Series supports Call Forward for host-controlled calls. When you enable DN Discovery, your Remote Gateway 9100 Series system supports Call Forward for locally controlled calls, as well.

Paging

When you press a local call appearance key, and then dial the Paging SPRE code, you can announce a page to all other stations at your site.

Note: You can disable Paging for any station.

Going online and offline

Stations at the Remote Gateway 9150 site operate in either online mode or offline mode. This is controlled by one or both of the following:

- SPRE codes to manually toggle all stations at your site between online and offline modes
- an online/offline schedule on the host PBX to automatically toggle all stations at your site between online and offline modes

For a description of the online and offline modes, refer to “Modes of operation” on page 260.

Using the SPRE code to put all stations into online mode

To use the SPRE code to put all stations into online mode:

- 1 Lift the digital telephone handset, or press one of the local call appearance keys.
- 2 Press the octothorpe key (# in North America) followed by the Online SPRE code.

Note: To learn this code, consult with your system administrator.

Result: The connection to the host PBX is initiated and negotiated with the host PBX. During this negotiation period (up to 5 seconds), stations at your site cannot be used for host-controlled calls. When negotiation is completed and connection to the host PBX has been established, Online Mode displays on the telephone display.

Using the SPRE code to put all stations into offline mode

To use the SPRE code to put all stations into offline mode:

- 1 Lift the digital telephone handset, or press one of the local call appearance keys.
- 2 Dial the pound key (# in North America) followed by the Offline SPRE code.

Note: To learn this code, consult with your system administrator.

Result: Offline Mode displays on the digital telephone set.

Overriding an automatic offline event from the host PBX

To override an automatic offline event from the host PBX:

If the host PBX attempts to process an offline event while you are on a host-controlled call, you are alerted by both an audible alert and a display message indicating that you are about to go offline in 30, 20, or 10 seconds. If you ignore this warning, your call will be disconnected.

To prevent your call from being disconnected, enter the online SPRE code. You can do this without putting your call on hold first. The online SPRE code cancels the offline event, leaving all stations online until the next offline event occurs.

Chapter 7

Administration

In this chapter

Changing the administration password	280
Creating a backup configuration file	282
Restoring the configuration	285
Display logs	290
Statistics screens	294
Verifying the firmware and software version	335
Obtaining the latest upgrade file	337
Performing a firmware upgrade	338
Performing a software upgrade	346

Changing the administration password

Two layers of password security protect the Remote Gateway 9150 unit's configuration. To secure the Remote Gateway 9150 unit's configuration so that only those with passwords unique to the unit can make configuration changes, alter the following items:

- Configuration Manager password
This password prevents unauthorized users from performing offline configuration changes.
- Remote Gateway 9150 unit's password
This password prevents unauthorized users from performing online changes of the configuration residing in the RLC's Flash memory.

Note: Nortel recommends that you change these passwords for logging on to both Configuration Manager and the Remote Gateway 9150 unit. Make sure that you record the password and store it in a safe, secure location. If you forget or lose the password, contact your Nortel customer support representative.

Getting there 9150 → Configuration Manager

Changing the Configuration Manager password

To change the Configuration Manager (local) password:

- 1 From the Menu Bar, choose Connect → Change Password → Local.

Result: The Change Password dialog box displays, similar to the following:

A screenshot of a Windows-style dialog box titled "Change Password - Local". The dialog box has a blue title bar with a close button (X) in the top right corner. Inside the dialog, there are three text input fields stacked vertically. The first field is labeled "Old Password", the second is labeled "New Password", and the third is labeled "Retype New Password". At the bottom of the dialog, there are two buttons: "OK" on the left and "Cancel" on the right.

- 2 Complete the fields in the Change Password dialog box.
- 3 Click on the **OK** button.

Result: The Password changed successfully dialog box displays.

- 4 Click on the **OK** button.

Changing the Remote Gateway 9150 unit password

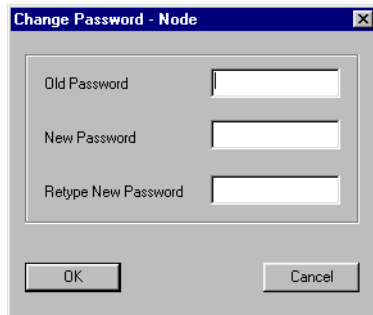
To change the Remote Gateway 9150 unit (node) password:

ATTENTION!

Do not change the Remote Gateway 9150 unit's password until the system is up and working.

- 1 From the Menu Bar, choose Connect → Change Password → Node.

Result: The Change Password displays, similar to the following:



- 2 Complete the fields in the Change Password dialog box.
- 3 Click on the **OK** button.

Result: The Board Password Changed Successfully dialog box displays.

Note: This means that Configuration Manager has written the password to the Remote Gateway 9150 unit's Flash memory.

- 4 Click on the **OK** button.
- 5 From the Menu Bar, choose Upload/Download → Save to Flash.

Result: Configuration Manager updates the Remote Gateway 9150 unit's memory with the new password.

- 6 Restart the Remote Gateway 9150 unit.

Creating a backup configuration file

Create a backup copy of the Remote Gateway 9150 unit's configuration by downloading the configuration from Flash memory to a text file on your administration PC. Nortel recommends that you create a backup of your configuration file whenever you make configuration changes or after you perform a firmware upgrade.

Storing backup configuration files

The Remote Gateway 9150 unit is an extension of the telecommunications and data network. It is extremely important that you keep a backup copy of the Remote Gateway 9150 unit's configuration. If the Remote Gateway 9150 unit's Flash memory or configuration becomes corrupted or is lost, you can easily restore it.

Store the configuration file in a safe, secure location, such as on backup tape or other media that is stored offsite.

Nortel recommends that you keep the backup files indefinitely.

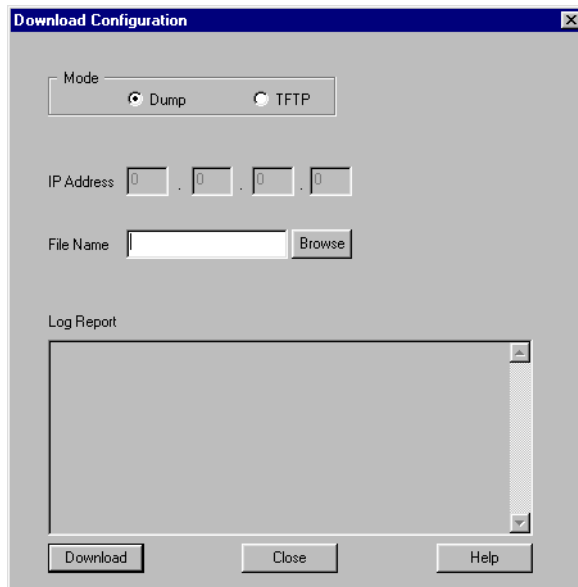
Getting there 9150 → Configuration Manager

Creating the backup file

To create the backup file:

- 1 From the Menu Bar, choose Upload/Download → Download Configuration.

Result: The Download Configuration dialog box displays, similar to the following:



- 2 Choose the mode you want to use for the file transfer according to the following table:

IF you wish to save the configuration file to

THEN do the following:

the administration PC,
a different location on the IP
network,

Click on the **Dump** option button.

- 1 Click on the **TFTP** option button.

Result: This enables the IP
Address fields.

- 2 Enter the IP address of the PC that
you want to save the configuration
file on.

- 3 Click on the **Browse** button and navigate to the folder where you want to keep the configuration text file.

- 4 Enter a name for the file in the File name field.

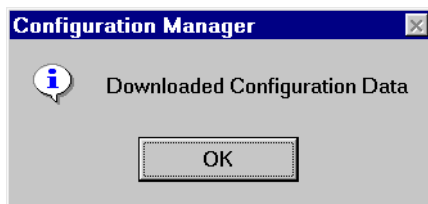
Note: This configuration file becomes your backup file, so ensure the file name is meaningful. The file name's extension must be .TXT.

- 5 Click on the **Download** button.

Result: The Download configuration dialog box closes, and the following message displays in the status bar at the bottom of the screen:

Downloading Config From Board

When the download is complete, the Downloaded Configuration Data dialog box displays, similar to the following:



- 6 Click on the **OK** button.

Note: Flash downloads to remote M39xx telephones can take twice as long compared to when these telephones are connected directly to a standard Nortel digital line card (XDLC).

Restoring the configuration

Restore the configuration to the Remote Gateway 9150 unit's Flash memory by uploading a configuration text file from a PC on the same network as the Remote Gateway 9150 unit. To do this, perform the upload over the IP network using the TFTP protocol.

Before you begin

Before you can upload the configuration file to the Remote Gateway 9150 unit, you must complete the following steps:

- 1 Start the TFTP server application.
- 2 Ensure that the TFTP base directory points to the location of the configuration file.

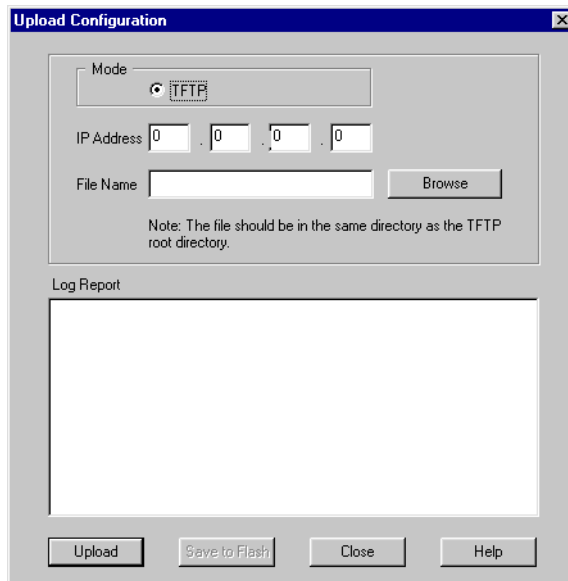
Getting there 9150 → Configuration Manager

Uploading a configuration file over the IP network

To upload a configuration file over the IP network:

- 1 From the Menu Bar, choose → Upload/Download → Upload Configuration.

Result: The Upload Configuration dialog box displays, similar to the following:



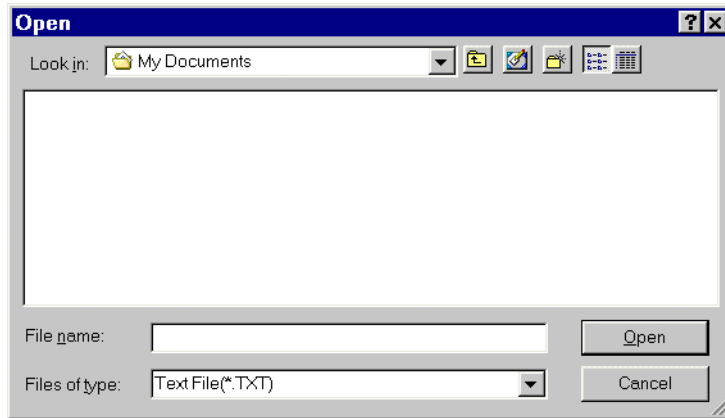
The screenshot shows a dialog box titled "Upload Configuration" with a standard Windows-style title bar (minimize, maximize, close buttons). The dialog has a light gray background. At the top, there is a "Mode" section with a radio button selected next to "TFTP". Below this is an "IP Address" field consisting of four small input boxes, each containing the digit "0". To the right of the IP address fields is a "Browse" button. Below the IP address fields is a "File Name" input field. A note below the File Name field states: "Note: The file should be in the same directory as the TFTP root directory." Below the note is a "Log Report" section with a large empty text area. At the bottom of the dialog are four buttons: "Upload", "Save to Flash", "Close", and "Help".

- 2 Enter the IP address of the TFTP server in the IP Address fields.

Note: Since the TFTP server application is running on your administration PC, this is the IP address of the administration PC.

- 3 Click on the **Browse** button.

Result: The Open dialog box displays, similar to the following:

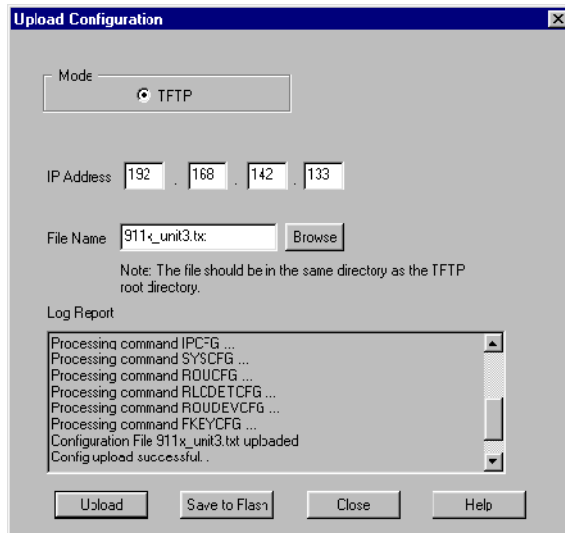


- 4 Ensure the Files of type drop down box shows Text File (*.TXT).
- 5 Navigate to the folder containing the configuration file.
- 6 Select the configuration file, and then click on the **Open** button.

Result: The Upload Configuration dialog box displays with the file you selected shown in the File Name field.

- 7 Click on the **Upload** button.

The middle of the Upload Configuration dialog box displays status messages relating to the upload. The following is an example.



CAUTION

Risk of incorrect operation due to partial configuration.

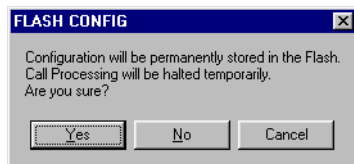
Do not interrupt the configuration upload. If you interrupt the configuration upload, this results in an incomplete configuration in the Remote Gateway 9150 unit's database.

If the configuration upload is interrupted, repeat this procedure immediately.

IF the upload	THEN
is successful,	<p>the following message displays:</p> <pre>CONFIG UPLOAD SUCCESSFUL... USE SAVECFG TO UPDATE FLASH.</pre> <p>Proceed to step 8.</p>
fails,	<p>the following message displays in the middle of the Upload Configuration dialog box:</p> <pre>CONFIG UPLOAD FAILED</pre> <p>For further instructions, refer to Chapter 8, "Troubleshooting."</p>

- 8 On the Upload Configuration dialog box, click on the **Save to Flash** button.

Result: The FLASH CONFIG dialog box displays, similar to the following:



- 9 Click on the **Yes** button.

Result: The following message displays in the status bar at the bottom of the screen:

Saving to Flash in Progress

When the save is finished, the following message displays in the middle of the Upload Configuration dialog box:

```
CONFIGURATION IS UPDATED INTO FLASH...
```

- 10 Click on the **Close** button.
- 11 Restart the Remote Gateway 9150 unit.

Note: For instructions, refer to "Performing a system restart or shutdown" on page 169.

Display logs

The Remote Gateway 9150 unit keeps track of system performance through the maintenance of display logs. Each line, or display log, represents a separate action completed by the unit. Refer to Appendix D, “Display log definitions,” or Configuration Manager online Help for a complete listing of all display logs and the condition indicated by each.

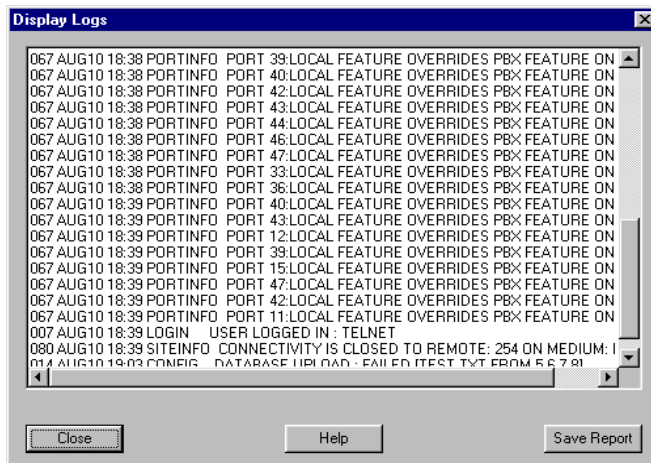
Use the display logs when troubleshooting system problems. Click on the **Save Report** button to print the display logs to a text file, or you can copy the information from the Display Logs window, and paste it into a text file.

Getting there 9150 → Configuration Manager

Viewing display logs

From the menu, choose Alarms/Stats/Logs → Display Logs.

Result: You can view the Remote Gateway 9150 unit's display logs in a window similar to the following. You can use the scroll bar to browse through the logs.

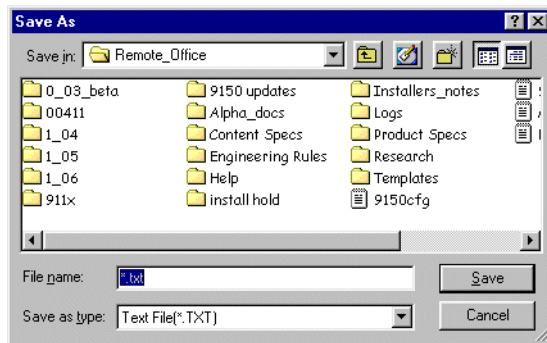


Printing the display logs to a file

If you request technical support, your support representative can ask you to provide a copy of the logs. To recreate the log in a file on your administration PC, follow this procedure:

- 1 After displaying the logs using the procedure explained under “Viewing display logs” on page 290, click on the **Save Report** button on the Display Logs window.

Result: The Save As dialog box displays, similar to the following:



- 2 Navigate to the folder where you want to store the log file.
- 3 Enter a name for the configuration in the File name field.
- 4 Click on the **Save** button.

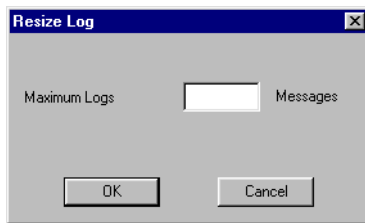
Result: Configuration Manager saves the logs to a text file in the location indicated in the Save As dialog box.

Changing the size of Remote Gateway 9150 unit logs

The Remote Gateway 9150 unit retains a maximum of 1000 display logs, each requiring one line of text. When the Remote Gateway 9150 unit's display logs reach 1000 lines, new display logs overwrite existing display logs on a first in, first out basis. If you want to change the number of display logs retained by the Remote Gateway 9150 unit:

- 1 From the Menu Bar, choose Alarms/Stats/Logs → Resize Logs.

Result: The Resize Log dialog box displays, similar to the following:



Note: "Maximum logs" refers to the number of text lines maintained in the Remote Gateway 9150 unit system log. The log holds a maximum of 1000 text lines, or the 1000 most recent display logs, when it shipped from the factory.

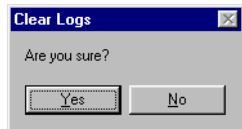
- 2 Enter the maximum number of display logs you want the Remote Gateway 9150 unit to keep in the Maximum Logs field.
- 3 Click on the **OK** button.

Clearing logs

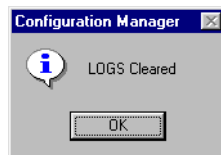
The Remote Gateway 9150 unit allows you to delete unneeded information by clearing the display logs that the Remote Gateway 9150 unit keeps. To discard or clear display logs that are no longer useful:

- 1 From the Menu Bar, choose Alarms/Stats/Logs → Clear Logs.

Result: The CLEAR LOGS dialog box displays, similar to the following:



IF you select	THEN
No,	the Clear logs dialog box closes and the logs remain as they are.
Yes,	<ul style="list-style-type: none">■ the Remote Gateway 9150 deletes its stored display logs.■ the LOGS cleared dialog box displays, similar to the following:



Click on the **OK** button.

Statistics screens

All statistics screens provided by the Alarms/Stats/Logs menu, function primarily to help you obtain information to provide to technical support personnel, upon request.

Getting there 9150 → Configuration Manager

Trunk Connection Statistics

Trunk Connection Statistics show you the PSTN trunk usage for the selected remote site, similar to the following:

[illegible]

To display the Trunk Connection Statistics screen, refer to “Displaying the Trunk Connection Statistics screen”. To obtain the definitions for the statistics presented on the Trunk Connection Statistics screen, refer to “Trunk Connection Statistics field descriptions” on page 296.

Displaying the Trunk Connection Statistics screen

Choose Alarms/Stats/Logs → Trunk Connection Statistics from the Menu Bar to display the Trunk Connection Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Trunk Connection Statistics screen, similar to the example on page 294.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Trunk Connection Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Trunk Connection Statistics screen,	on the Help button.

Trunk Connection Statistics field descriptions

The following table describes the statistics on the Trunk Connection Statistics screen:

Statistic	Description
Trunk Number	RLC - Identifies the Network Port number used for the call. The third pair of numbers (the third item in the triplet) corresponds to the port on the RLC. 9150 - Identifies the ISDN BRI module and B-channel used for the call. 911x - Identifies the only trunk available to the remote unit with all zeroes.
Status	Identifies the current status of the trunk. Valid values are Active and Idle.
Call Type	Identifies whether the call is a local call or a remote signaling call. Valid values are Local and Signaling.
Remote ID	Identifies the remote unit involved in the call.
Called Number	Identifies the remote DN regardless of who initiated the call.
Start Time	Identifies the time that the last call on this trunk began.
Close Time	Identifies the time that the last call on this trunk ended. If the trunk is active, this statistic displays "NA".
Duration	Identifies the amount of time taken for the call.

Bandwidth Connection Statistics

Bandwidth Connection Statistics allow you to see how much bandwidth is actually being used. These statistics help you determine if you need to add more bandwidth on the PSTN or IP network connections. They show the amount of bandwidth all remote units connected to the logged-on RLC have available to them, similar to the following:

Remote Unit Number	Signaling Status	No of Voice Calls on IP	No of Voice Calls on PSTN	Used IP BW	Used Trunk
254	IDLE	0	0	0.00	0.00

Refresh Save to File Close Reset Help

To display the Bandwidth Connection Statistics screen, refer to “Displaying the Bandwidth Connection Statistics screen” on page 298. To obtain the definitions for the statistics presented on the Bandwidth Connection Statistics screen, refer to “Bandwidth Connection Statistics field descriptions” on page 299.

Displaying the Bandwidth Connection Statistics screen

Choose Alarms/Stats/Logs → BW Connection Statistics from the Menu Bar to display the Bandwidth Connection Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Bandwidth Connection Statistics, similar to the example on page 297.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Bandwidth Connection Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Bandwidth Connection Statistics screen,	on the Help button.

Bandwidth Connection Statistics field descriptions

The following table describes the statistics on the Bandwidth Connection Statistics screen:

Column	Description
Remote Unit Number	Identifies the remote unit that initiated the call.
Signaling Status	Identifies whether a connection is up on this unit. Valid values are Active and Idle.
No of Voice Calls on IP	Identifies the number of calls in progress on this unit's IP connection.
No of Voice Calls on PSTN	Identifies the number of calls in progress on this unit's PSTN connection.
Used IP BW	Identifies the IP bandwidth in use on this unit.
Used Trunk BW	Identifies the PSTN bandwidth in use on this unit.
Total Up Trunk BW	Identifies the total PSTN bandwidth up and available to this unit.
IP QoS Status	Identifies the Quality of Service (QoS) level on this unit's IP connection. Valid values are Good and Bad.

Caller Info Statistics

Caller Info (Information) Statistics show you the types of calls being made (IP or PSTN) and how often QoS transitions occur. Use these statistics to help you determine if voice QoS on your IP network is stable. The Caller Info Statistics screen is similar to the following:

[illegible]

To display the Caller Info Statistics screen, refer to “Displaying the Caller Info Statistics screen” on page 301. To obtain the definitions for the statistics presented on the Caller Info Statistics screen, refer to “Caller Info Statistics field descriptions” on page 302.

Displaying the Caller Info Statistics screen

Choose Alarms/Stats/Logs → Caller Info Statistics from the Menu Bar to display the Caller Info Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Caller Info Statistics screen, similar to the example on page 300.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Caller Info Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Caller Info Statistics screen,	on the Help button.

Caller Info Statistics field descriptions

The following table describes the statistics on the Caller Info Statistics screen:

Column	Description
Connection ID	Identifies the sequential number of the call processed by the remote unit in relation to all calls ever processed by that unit.
Remote ID	Identifies the Unit ID of the remote site that was involved in the call. Local calls on a Remote Gateway 9150 unit result in a 0 in this field.
Current Media	Identifies whether the call took place over the PSTN or IP network.
Type	Identifies the type of call. Valid values are Signaling, Voice, and Local.
Priority	Identifies the priority setting of the involved trunk. Valid values are PSTN Only, IP Only, High, and Normal.
Call BW	Identifies the amount of bandwidth used by the call.
Start Time	Identifies the time that the connection initiated.
Transitions to PSTN	Identifies the number of times the RLC moved the call to the PSTN.
Transitions to IP	Identifies the number of times the RLC moved the call to the IP network.
Last Transition to PSTN	Identifies the last time the RLC moved the call from the IP network to the PSTN.
Last Transition to IP	Identifies the last time the RLC moved the call from the PSTN to the IP network.

Hardware Statistics

Hardware Statistics provide information concerning the trunk interface or DSP application modules that are installed on the logged-on Remote Gateway 9150 unit. Use these statistics to determine which module positions are populated and the type of modules present in those positions. The Hardware Statistics screen is similar to the following:

[illegible]

To display the Hardware Statistics screen, refer to “Displaying the Hardware Statistics screen” on page 305. To obtain the definitions for the statistics presented on the Hardware Statistics screen, refer to “Hardware Statistics field descriptions” on page 306.

Information concerning the trunk interface and DSP application modules that are installed on the Remote Gateway 9150 unit also displays in the Startup Information dialog box. This dialog box includes the following information:

The column	contains the following information:
SLOTNO	the slot number occupied by the application module. Valid options are 1, 2, 3, and 4.
STATUS	whether the slot contains a functioning DSP application module. Valid options are: <ul style="list-style-type: none">■ EQUIPPED—a working DSP application module is in the slot■ OUT SERVICE—a faulty application module is in the slot■ UNEQUIPPED—no application module is in the slot
TYPE	the type of application module in the slot.
VERSION	the version of application module in the slot.

This dialog box displays as a result of a successful attempt to log on to a particular Remote Gateway 9150 unit. You can locate the information contained in the preceding table by using the scroll bar available in the System Information section of the dialog box. Refer to page 160 for further details.

Displaying the Hardware Statistics screen

Choose Alarms/Stats/Logs → Hardware Statistics from the Menu Bar to display the Hardware Statistics screen:

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Hardware Statistics screen, similar to the example on page 303.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Hardware Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Hardware Statistics screen,	on the Help button.

Hardware Statistics field descriptions

The following table describes the statistics on the Hardware Statistics screen:

Column	Description
Module No	Identifies the DSP application module's position on the Remote Gateway 9150 or RLC motherboard.
Status	Identifies whether there is a functional DSP application module in the position identified in the Module No field. Valid values are Equipped and Unequipped. Equipped means that a DSP application module is installed in the module position and Unequipped means that there is not a DSP application module installed in the module position.
Module Type	Identifies the part number of the hardware installed in the module position.
Version	Identifies the version of DSP application module installed in the module position.

DSP Statistics

DSP Statistics provide information about the DSP application modules installed on the logged-on Remote Gateway 9150 unit. Use this screen to determine the module positions that are populated, what type of DSP those positions contain, and the functionality provided by each. The DSP Statistics screen is similar to the following:

[illegible]

To display the DSP Statistics screen, refer to “Displaying the DSP Statistics screen” on page 308. To obtain the definitions for the statistics presented on the DSP Statistics screen, refer to “DSP Statistics field descriptions” on page 309.

Displaying the DSP Statistics screen

Choose Alarms/Stats/Logs → DSP Statistics from the Menu Bar to display the DSP Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the DSP Statistics screen, similar to the example on page 307.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the DSP Statistics screen,	on the Close button.
obtain descriptions of the statistics in the DSP Statistics screen,	on the Help button.

DSP Statistics field descriptions

The following table describes the statistics on the DSP Statistics screen:

Column	Description
Single Digit Device ID	Identifies an internal sequence number for indexing this DSP device among all others on the RLC.
Module Number	Identifies this DSP Application Module's module number on the Remote Gateway 9150 unit. Valid values are 0, 1, 2, and 3.
Device Number	Identifies the DSP device that processed the call.
In Service	Identifies any voice channels operating on this DSP application module.
Total MIPS	Identifies the total millions of instructions per second (MIPS) capacity for this DSP device.
Available Mips	Identifies the millions of instructions per second (MIPS) currently available on this DSP device.
Total Channels	Identifies the total channel capacity for this DSP device.
Total Voice Channels	Identifies the total voice channel capacity for this DSP device.
Available Voice Channels	Identifies the number of unused voice channels on this DSP device.
Total Modem Channels	Identifies the number of channels on this DSP device that can transmit modem calls.
Available Modem Channels	Identifies the number of unused channels on this DSP that can transmit modem calls.
Total Flex Channels	Identifies the number of channels on this DSP that can provide multiple functionalities.
Available Flex Channels	Identifies the number of channels on this DSP currently available to provide multiple functionalities.

Column	Description
Total Tones Channels	Identifies the number of channels on this DSP that can transmit tones.
Total Reserved Channels	Identifies the number of special purpose channels on this DSP reserved for internal use.
Name	Identifies the name of the DSP load, that is, the combination of DSP algorithms, on the DSP application module.

Ethernet Interface Statistics

Ethernet Interface Statistics provide information about the connection between the IP network and the logged-on Remote Gateway 9150 unit that is achieved over the Remote Gateway 9150 unit's Ethernet interface. The Ethernet Interface Statistics screen is similar to the following:

[illegible]

To display the Ethernet Interface Statistics screen, refer to “Displaying the Ethernet Interface Statistics screen” on page 312. To review the definitions for the statistics presented on the Ethernet Interface Statistics screen, refer to “Ethernet Interface Statistics field descriptions” on page 313.

Displaying the Ethernet Interface Statistics screen

Choose Alarms/Stats/Logs → Ethernet Interface Statistics from the Menu Bar to display the Ethernet Interface Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Ethernet Interface Statistics screen, similar to the example on page 311.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Ethernet Interface Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Ethernet Interface Statistics screen,	on the Help button.

Ethernet Interface Statistics field descriptions

The following table describes the statistics found on the Ethernet Interface Statistics screen:

Column	Description
Channel	Identifies the Ethernet device that the statistics on that line apply to. The valid values are is1.
LAN Drv	Identifies the LAN driver used by the call.
Admin	Identifies the administrative state of the port. Valid values are 1 (Enabled) and 0 (Disabled).
Oper	Identifies the operational state of the port. Valid values are 1 (Up) and 0 (Down).
IfcType	Identifies the interface type used by the call.
IfcNo	Identifies the Ethernet interface used by the call. The valid value is 1 (CLAN).
MTUlen	Identifies the Maximum Transmission Unit for this interface in bytes.
Speed	Identifies the data rate of this interface in Mbps.
Rx Octet	Identifies the number of bytes received on the given channel since the statistics were last reset.
Rx Ucast	Identifies the number of packets with a unicast Ethernet address that directly matches the Ethernet address of the identified unit. This statistic describes the period of time since the statistics were last reset.
Rx Mcast	Identifies the number of multicast packets received. These packets can be broadcast MAC addresses for protocols such as ARP, as well as multicast packets for group-oriented transmissions such as IP Multicast. This statistic describes the period of time since the statistics were last reset.

Column	Description
Rx Disc	Identifies the number of packets discarded on the channel since the statistics were last reset.
Rx Err	Identifies the number of error packets received on the given channel since the statistics were last reset.
Tx Octet	Identifies the number of outbound bytes transmitted on the given channel since the statistics were last reset.
Tx Ucast	Identifies the number of outbound packets sent to a Unicast Address (single recipient) on the given channel since the statistics were last reset.
Tx Mcast	Identifies the number of outbound packets sent to multiple recipients on the given channel since the statistics were last reset.
Tx Disc	Identifies the number of outbound packets discarded due to resource problems on the given channel since the statistics were last reset.
Tx Err	Identifies the number of outbound packets discarded due to errors on the given channel since the statistics were last reset.
QLen	Identifies the number of bytes currently in the interface's outbound queue.
Collisions	<p>Identifies the number of collisions that have occurred on the Ethernet interface while attempting to transmit packets since the statistics were last reset.</p> <p>Note: The Collisions statistic appears on both the Ethernet Interface and Network Statistics screens. The Collisions statistic is only applicable in half-duplex mode.</p>

BRI Information Statistics

BRI Information Statistics provide information about the BRI modules installed on the logged-on Remote Gateway 9150 unit. Use this screen to determine the module positions that are populated, the type and status of each module, the number of BRI channels available and being used, and the cross-connections being used. The BRI Information Statistics screen is similar to the following:

[illegible]

To display the BRI Information Statistics screen, refer to “Displaying the BRI Information Statistics screen” on page 316. To review the definitions for the statistics presented on the BRI Information Statistics screen, refer to “BRI Information Statistics field descriptions” on page 317.

Displaying the BRI Information Statistics screen

Choose Alarms/Stats/Logs → BRI Statistics from the Menu Bar to display the BRI Information Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the BRI Information Statistics screen, similar to the example on page 315.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the BRI Information Statistics screen,	on the Close button.
obtain descriptions of the statistics in the BRI Information Statistics screen,	on the Help button.

BRI Information Statistics field descriptions

The following table describes statistics found on the BRI Information Statistics screen:

Column	Description
Module Index	Identifies the port where the call originated. Valid values are 0 through 63.
Module Number	Identifies the module position of the ISDN BRI module that handled the call. Valid values are 4, 5, 6, and 7.
Device Number	Identifies internal sequence number for indexing ISDN BRI devices.
In Service	Indicates the successful initialization of the ISDN BRI module.
Usage	Bit-encoded field identifies the module as an ISDN BRI module.
Total Channels	Identifies the ISDN BRI module's working and non-working channels.
Available Channels	Identifies the working channels on the ISDN BRI module.
Cross Connection Type	Identifies the cross-connect type used by the ISDN BRI module. Valid values are DS30X, AMB, REG, and VHD.
Name	Identifies the type and version of the ISDN BRI module that handled the call.

Local Call Statistics

The Local Call Statistics screen allows you to see how many local calls the Remote Gateway 9150 unit processes through the local PSTN and how long these calls last. The Local Call Statistics screen is similar to the following:

Port No	Call Start Time	Call Duration
7	NA	NA

To display the Local Call Statistics screen, refer to “Displaying the Local Call Statistics screen” on page 319. To obtain the definitions for the statistics presented on the Local Call Statistics screen, refer to “Local Call Statistics field descriptions” on page 319.

Displaying the Local Call Statistics screen

Choose Alarms/Stats/Logs → Local Call Stats from the Menu Bar to display the Local Call Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Local Call Statistics screen, similar to the example on page 318.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Local Call Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Local Call Statistics screen,	on the Help button.

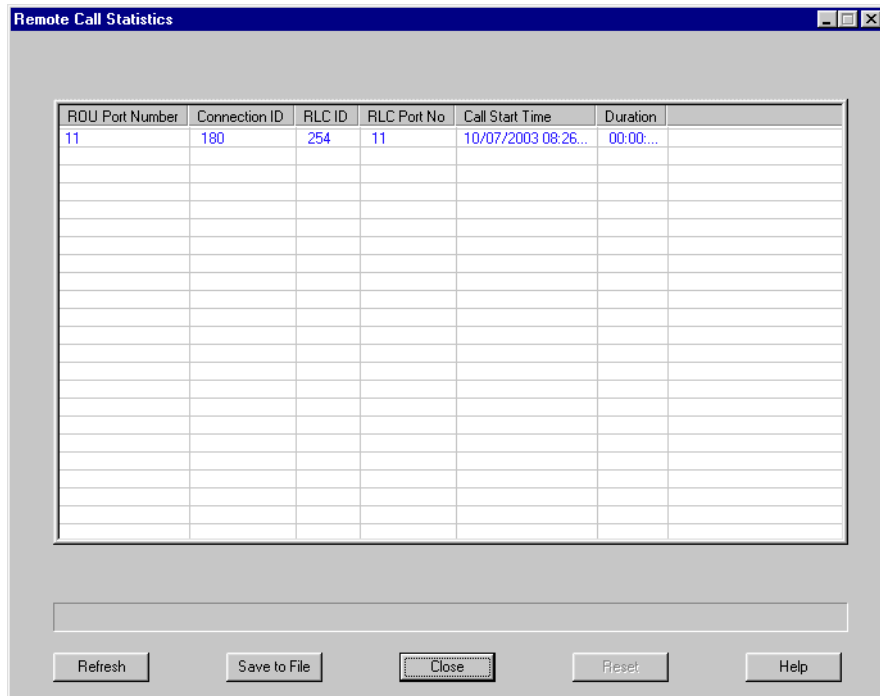
Local Call Statistics field descriptions

The following table describes the statistics found on the Local Call Statistics screen:

Column	Description
Port No.	Identifies the Remote Gateway 9150 port that processed the call.
Call Start Time	Identifies the time when the call started.
Call Duration	Identifies the length of the call.

Remote Call Statistics

The Remote Call Statistics screen allows you to see how many calls the Remote Gateway 9150 unit processes through the host PBX. This screen shows which ports handle the calls, and how long each call lasts. Use this statistics log to determine how much host PBX traffic the Remote Gateway 9150 unit processes. The Remote Call Statistics screen is similar to the following:



To display the Remote Call Statistics screen, refer to “Displaying the Remote Call Statistics screen” on page 321. To review the definitions for the statistics presented on the Remote Call Statistics screen, refer to “Remote Call Statistics field descriptions” on page 321.

Displaying the Remote Call Statistics screen

Choose Alarms/Stats/Logs → Remote Call Stats from the Menu Bar to display the Remote Call Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Local Call Statistics screen, similar to the example on page 320.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Remote Call Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Remote Call Statistics screen,	on the Help button.

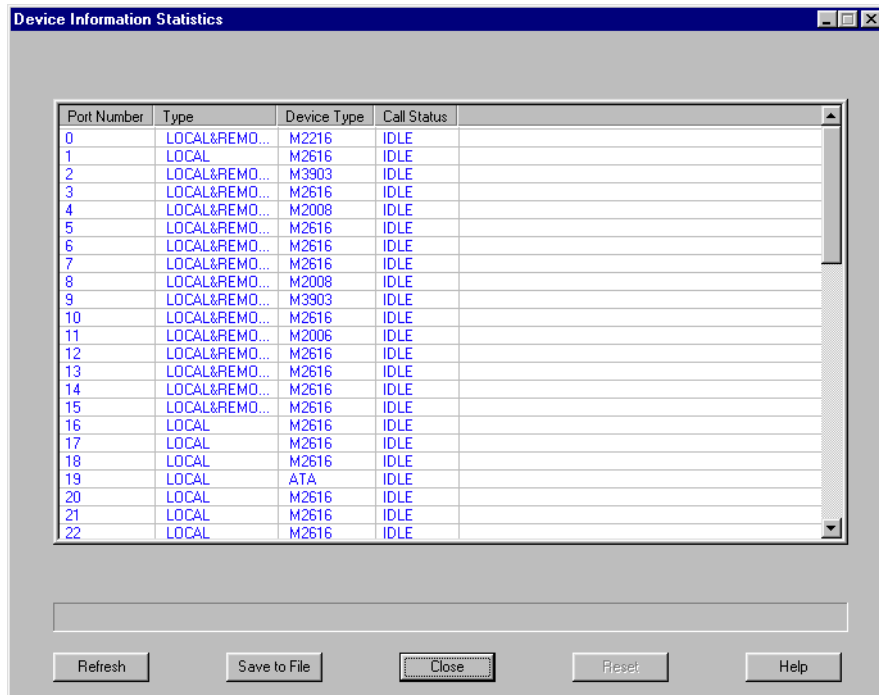
Remote Call Statistics field descriptions

The following table describes the statistics found on the Remote Call Statistics screen:

Column	Description
ROU (Remote Gateway 9150) Port No	Identifies the Remote Gateway 9150 port that processed the call.
Connection ID	A sequential number used for tracking individual calls.
RLC ID	Identifies the Unit ID of the RLC that processed the call.
RLC Port No	Identifies the RLC port that processed the call.
Call Start Time	Identifies the time when the call began.
Duration	Identifies how long the call lasted.

Device Information Statistics

The Device Information Statistics screen allows you to see all telephones connected to the Remote Gateway 9150 unit, their capability, and current status. The Device Information Statistics screen is similar to the following:



The screenshot shows a window titled "Device Information Statistics" with a table of device information. The table has four columns: Port Number, Type, Device Type, and Call Status. The data is as follows:

Port Number	Type	Device Type	Call Status
0	LOCAL&REMO...	M2216	IDLE
1	LOCAL	M2616	IDLE
2	LOCAL&REMO...	M3903	IDLE
3	LOCAL&REMO...	M2616	IDLE
4	LOCAL&REMO...	M2008	IDLE
5	LOCAL&REMO...	M2616	IDLE
6	LOCAL&REMO...	M2616	IDLE
7	LOCAL&REMO...	M2616	IDLE
8	LOCAL&REMO...	M2008	IDLE
9	LOCAL&REMO...	M3903	IDLE
10	LOCAL&REMO...	M2616	IDLE
11	LOCAL&REMO...	M2006	IDLE
12	LOCAL&REMO...	M2616	IDLE
13	LOCAL&REMO...	M2616	IDLE
14	LOCAL&REMO...	M2616	IDLE
15	LOCAL&REMO...	M2616	IDLE
16	LOCAL	M2616	IDLE
17	LOCAL	M2616	IDLE
18	LOCAL	M2616	IDLE
19	LOCAL	ATA	IDLE
20	LOCAL	M2616	IDLE
21	LOCAL	M2616	IDLE
22	LOCAL	M2616	IDLE

Below the table is a search bar and a set of buttons: Refresh, Save to File, Close, Reset, and Help.

To display the Device Information Statistics screen, refer to “Displaying the Device Information Statistics screen” on page 323. To review the definitions for the statistics presented on the Device Information Statistics screen, refer to “Device Information Statistics field descriptions” on page 324.

Displaying the Device Information Statistics screen

Choose Alarms/Stats/Logs → Device Information to display the Device Information Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Device Information Statistics screen, similar to the example on page 322.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Device Information Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Device Information Statistics screen,	on the Help button.

Device Information Statistics field descriptions

The following table describes the statistics found on the Device Information Statistics screen:

Column	Description
Port Number	Identifies the Remote Gateway 9150 unit port number associated with the displayed information.
Type	Identifies the port type. Valid values are Remote, Data, and Local TCM.
Device Type	Identifies whether the telephone connection on the port identified above is Normal or ACD. Valid values are Normal and ACD.
Call Status	Identifies whether the port is currently handling a call. Valid values are Busy and Idle.
Login Status	Identifies whether the telephone connected to this port is active on the system. Valid values are Logged on and Logged off. Note: This statistic applies only to ports associated with ACD telephones.

ISDN Module Information Statistics

The ISDN Module Information Statistics screen allows you do review the current status of the ISDN BRI modules on your Remote Gateway 9150 unit. The ISDN Module Information Statistics screen is similar to the following.

[illegible]

To display the ISDN Module Information Statistics screen, refer to “Displaying the ISDN Module Information Statistics screen” on page 326. To review the definitions for the statistics presented on the ISDN Module Information Statistics screen, refer to “ISDN Module Information field descriptions” on page 326.

Displaying the ISDN Module Information Statistics screen

Choose Alarms/Stats/Logs → ISDN Module Information to display the ISDN Module Information Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the ISDN Module Information Statistics screen, similar to the example on page 325.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the ISDN Module Information Statistics screen,	on the Close button.
obtain descriptions of the statistics in the ISDN Module Information Statistics screen,	on the Help button.

ISDN Module Information field descriptions

The following table describes statistics found on the ISDN Module Information Statistics screen:

Column	Description
Module Number	Identifies the module position of the ISDN BRI module. Valid values are 4, 5, 6, and 7.
Module Type	Identifies the type of the ISDN BRI module. Valid values are BRI-U, BRI-ST, and INVALID.
Link Status	Identifies the current status of the ISDN BRI line. Valid values are UP, DOWN, and INVALID.
Usage	Identifies whether the ISDN BRI line is in use or not. Valid values are IDLE and ACTIVE.

Network Statistics

Network Statistics allow you to see the performance over the last 24 hours of the logged-on Remote Gateway 9150 unit. Use these statistics to identify periods when other network activity can adversely affect 9150 system performance. This screen shows Remote Gateway 9150 unit performance in terms of the transmission and reception of frames and packets, similar to the following.

Network Statistics

Remote Unit Number = 254 IP Address : 192.168.143.230

Hour	Tx Voice Samples	Rx Voice Samples	Rx Error	Rx Dropped	% Error	EthTx Mcast	EthTx Ucast	EthTx
0	34575	36507	0	3	0.01 ...	0	13802	0
1	0	0	0	0	0.00 ...	0	948	0
2	0	0	0	0	0.00 ...	0	966	0
3	0	0	0	0	0.00 ...	0	970	0
4	0	0	0	0	0.00 ...	0	994	0
5	0	0	0	0	0.00 ...	0	967	0
6	0	0	0	0	0.00 ...	0	966	0
7	0	0	0	0	0.00 ...	0	971	0
8	0	0	0	0	0.00 ...	0	949	0
9	0	0	0	0	0.00 ...	0	1009	0
10	0	0	0	0	0.00 ...	0	955	0
11	45900	23583	0	0	0.00 ...	0	17066	0
12	16386	11148	0	3	0.03 ...	0	6740	0
13	0	0	0	0	0.00 ...	0	1046	0
14	0	0	0	0	0.00 ...	0	957	0
15	0	3	0	0	0.00 ...	0	1456	0
16	7266	9369	0	0	0.00 ...	0	3958	0
17	27453	28290	0	0	0.00 ...	0	10449	0
18	60771	90450	0	0	0.00 ...	0	23429	0
19	22926	13515	0	0	0.00 ...	0	9124	0
20	4302	6102	0	0	0.00 ...	0	2631	0
21	25335	51495	0	0	0.00 ...	0	10814	0

Refresh Save to File Close Reset Help

To display the Network Statistics screen, refer to “Displaying the Network Statistics screen” on page 328. To review the definitions for the statistics presented on the Network Statistics screen, refer to “Network Statistics field descriptions” on page 329.

Displaying the Network Statistics screen

Choose Alarms/Stats/Logs → Network Statistics from the Menu Bar to display the Network Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the Network Statistics screen, similar to the example on page 327.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Network Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Network Statistics screen,	on the Help button.

Network Statistics field descriptions

The following table describes the statistics found on the Network Statistics screen:

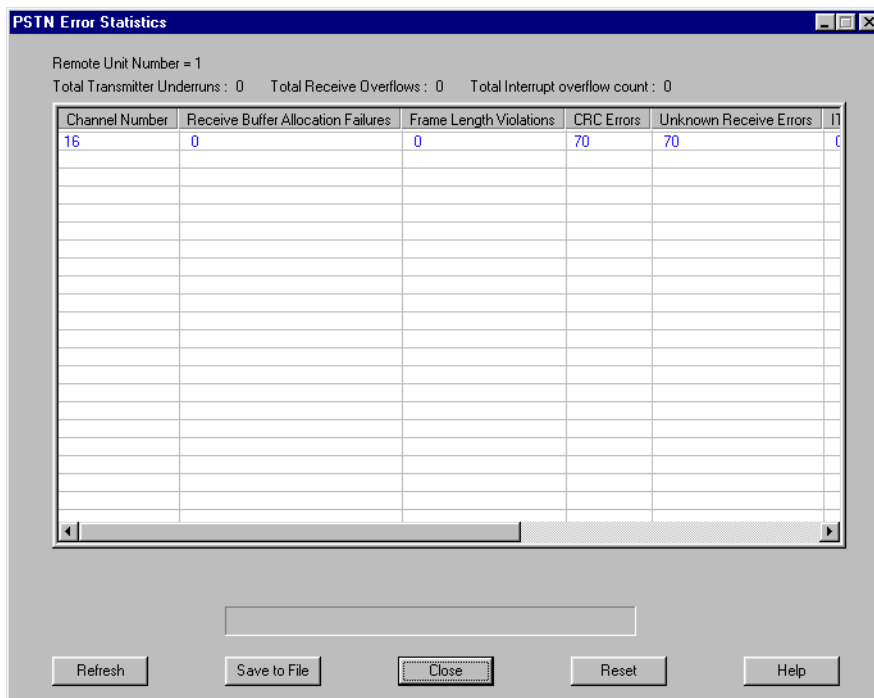
Statistic	Description
Hour	Identifies the 60-minute period, within the most recent 24 hours, that the other statistics on this line apply to. The statistics on the line where "0" is in this column refer to activity that occurred within 60 minutes of the request for statistics. The statistics on the line where "1" is in this column refer to activity that occurred during the 60-minute period that ended 60 minutes, or one hour, before the request for statistics. The statistics on the line where "2" is in this column refer to activity that occurred during the 60-minute period that ended two hours before the request for statistics, and so on.
Tx Voice Samples	Identifies the number of decoder packets transmitted by the DSP during the given hour. This number corresponds to in-band signaling, such as DTMF or Fax Relay, and voice signaling transmitted by the DSP. Note: This statistic formerly was expressed in superpackets rather than decoder packets.
Rx Voice Samples	Identifies the number of decoder packets received by the DSP during the given hour. This number corresponds to in-band signaling, such as DTMF or Fax Relay, and voice signaling received by the DSP. Note: This statistic formerly was expressed in superpackets rather than decoder packets.
Rx Error	Identifies the number of decoder packet overruns and underruns during the given hour, as determined by the DSP.
Rx Dropped	Identifies the number of superpackets that were received out of sequence during the given hour. This can result from one or more superpacket's being lost or delivered out of order and, thus, discarded.

Statistic	Description
%Error	<p>Identifies the packet error percentage that was received during the given hour.</p> <p>Remote Gateway 9100 Series begins calculating this statistic by adding the number out-of-sequence packets (Rx Dropped) to the number of overruns. After multiplying this sum by 100, Remote Gateway 9100 Series then divides the product by the number of received decoder packets (Rx Voice Samples) to produce the error percentage.</p> <p>This is an imprecise measurement due to the fact that multiple packet losses or overruns can be counted as a single error.</p>
EthTx Mcast	<p>Identifies the number of multicast packets transmitted during the given hour.</p> <p>Multicast packets are packets intended for multiple Ethernet addresses.</p>
EthTX Ucast	<p>Identifies the number of unicast packets transmitted during the given hour.</p> <p>Unicast packets are packets intended for a specific Ethernet address. Voice packets are always transmitted as unicast packets.</p>
EthTx Disc	<p>Identifies the number of packets discarded on the transmit side due to lack of resources, such as memory buffers, during the given hour.</p> <p>This can be an indirect result of excessive collisions in the transmit queue.</p>
EthRx Mcast	<p>Identifies the number of multicast packets that were received during the given hour. This is inclusive of packets with broadcast MAC addresses for protocols such as ARP, and multicast packets for group-oriented transmissions, such as IP Multicast.</p> <p>Multicast packets are packets intended for more than one Ethernet address.</p>

Statistic	Description
EthRx UCast	Identifies the number of unicast packets that were received during the given hour with a unicast Ethernet address directly matching that of the specified unit. Unicast packets are packets intended for only one Ethernet address.
EthRx Disc	Identifies the number of packets that were received during the given hour and discarded due to a lack of available receive buffers.
EthTx Err	Identifies the number of packets that could not be transmitted because of errors within the packets.
EthRx Err	Identifies the number of packets that were received during the given hour that contained errors that prevented them from being deliverable to a higher-layer protocol.
Collisions	Identifies the number of collisions that have occurred on the Ethernet interface when attempting to transmit packets since the statistics were last reset. Note: The Collisions statistic appears on both the Ethernet Interface and Network Statistics screens. The Collisions statistic is only applicable in half-duplex mode.

PSTN Error Statistics

PSTN Error Statistics allow you to see the PSTN performance, in terms of signaling errors, of digital telephone sets connected to the logged-on Remote Gateway 9150 unit. Use these statistics to gauge the effectiveness of your connection to the PSTN. The table displays error totals for all active PSTN calls placed from your Remote Gateway 9150 unit, similar to the following.



Remote Unit Number = 1

Total Transmitter Underruns : 0 Total Receive Overflows : 0 Total Interrupt overflow count : 0

Channel Number	Receive Buffer Allocation Failures	Frame Length Violations	CRC Errors	Unknown Receive Errors	
16	0	0	70	70	11

Refresh Save to File Close Reset Help

Displaying the PSTN Error Statistics screen

Choose Alarms/Stats/Logs → PSTN Error Statistics from the Menu Bar to display the PSTN Error Statistics screen.

Result: Configuration Manager gathers statistics from the Remote Gateway 9150 unit and displays the PSTN Error Statistics screen, similar to the example on page 332.

IF you want to	THEN click on the
update the statistics by adding PSTN error information that occurred since your original request,	Refresh button.
create a text file containing these statistics,	Save to File button.
close the PSTN Error Statistics screen,	Close button.
begin collecting new statistics,	Reset button.
obtain descriptions of the statistics in the PSTN Error Statistics screen,	Help button.

PSTN Error Statistics field descriptions

The following table describes the information on the PSTN Error Statistics screen:

Statistic	Description
Channel Number	Identifies the channel that the statistics on that line apply to.
Receive Buffer Allocation Failures	Identifies the number of times since the statistics were last reset that there was an error in the allocation of a packet to the receive buffer.
Frame Length Violations	Identifies the number of times since the statistics were last reset that a frame contained too many packets.
CRC Errors	<p>Identifies the number of times since the statistics were last reset that the cyclic redundancy check (CRC) bits did not match.</p> <p>The CRC errors that Trunk Protocol reports on the Remote Gateway 9100 Series product are check performed end-to-end at the High-level Data Link Control (HDLC) framing level. This check includes the ISDN framing errors as well as PSTN spans and clocking issues. The CRC error count does not always indicate that there are CRC errors on the physical line between the Remote Gateway 9150 unit and the CO, or the host PBX and the CO. However, the CRC error count is a good indication that you need to investigate the physical line.</p>
Unknown Receive Errors	Identifies the number of times since the statistics were last reset that a receive error that is not otherwise classified in this display occurred.
ITE Frame Length Violations	Identifies the number of times since the statistics were last reset that the ITE received an over-length frame.
ITE Transmitter Underruns	Identifies the number of times since the statistics were last reset that the ITE transmitter contained underruns.
ITE Receiver Busy Errors	Identifies the number of times since the statistics were last reset that the ITE received busy errors.

Verifying the firmware and software version

This section describes how to determine the version of firmware and software currently installed.

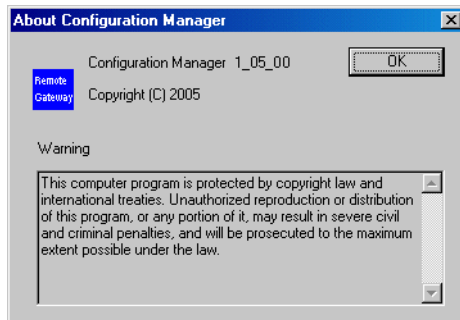
Before you perform a firmware or software upgrade, determine what version is currently installed. This ensures that you do not replace the installed firmware or software with an older version.

Verifying the software version

To verify the software version on your Remote Gateway 9150 unit:

- 1 From the Menu Bar, choose Help → About Configuration Manager.

Result: The About Configuration Manager dialog box displays, similar to the following:



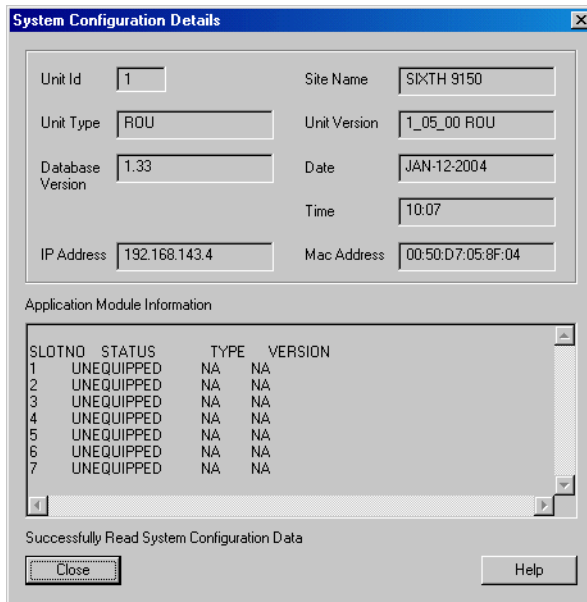
- 2 Review the About Configuration Manager dialog box. This identifies the version of software installed on the unit.
- 3 Click on the **OK** button.

Verifying the firmware version

To verify the firmware version on your Remote Gateway 9150 unit:

- 1 From the Menu Bar, choose System Information → System Data.

Result: The System Configuration Details dialog box displays, similar to the following:



The dialog box titled "System Configuration Details" contains the following fields and information:

Field	Value
Unit Id	1
Site Name	SIXTH 9150
Unit Type	ROU
Unit Version	1_05_00 ROU
Database Version	1.33
Date	JAN-12-2004
Time	10:07
IP Address	192.168.143.4
Mac Address	00:50:D7:05:8F:04

Application Module Information

SLOTNO	STATUS	TYPE	VERSION
1	UNEQUIPPED	NA	NA
2	UNEQUIPPED	NA	NA
3	UNEQUIPPED	NA	NA
4	UNEQUIPPED	NA	NA
5	UNEQUIPPED	NA	NA
6	UNEQUIPPED	NA	NA
7	UNEQUIPPED	NA	NA

Successfully Read System Configuration Data

Buttons: Close, Help

- 2 Review the Unit Version field. This identifies the version of firmware installed on the unit.
- 3 Click on the **Close** button.

Determining the current firmware and software versions

To determine the current firmware and software versions, refer to the *Remote Gateway 9100 Series and RLC Release Notes* (NTP 555-8421-102).

Obtaining the latest upgrade file

If you need to upgrade the firmware or software, you can obtain the latest upgrade files by clicking on the Software Downloads link at the following website:

www.nortel.com

Nortel provides upgrade files in self-extracting executable files. You must extract the upgrade files before you can perform the upgrade.

Types of upgrades

You can perform the following types of upgrades for your Remote Gateway 9150 unit:

- Configuration Manager software upgrade
 - firmware upgrades
 - Remote Gateway 9150 motherboard firmware

Note: This includes any firmware updates that have been made for DSP application modules.
 - trunk interface module firmware
- The firmware contains the code necessary for operating the Remote Gateway 9150 unit.

Downloading the upgrade file

To download the upgrade file:

- 1 With your web browser, connect to the Nortel web site at:
www.nortel.com
- 2 Click on the **Software Downloads** link.
- 3 Locate the software and firmware you need.
- 4 Download the files into a temporary location on your PC.
- 5 Double-click on the **.exe** file to extract the files into a temporary location on your PC.

Performing a firmware upgrade

This section describes how to perform a firmware upgrade on your Remote Gateway 9150 unit. You perform the upgrade over the IP network using the TFTP protocol. You can perform the RLC upgrade manually or configure the RLC to perform an automatic or scheduled firmware upgrade. Refer to “Auto upgrade configuration” on page 243 for further details.

Note: Over an IP network with low delay and packet loss, Flash download times to remote M39xx digital telephone sets are comparable to PBX wired downloads. Download times increase when you use PSTN bandwidth on a Remote Gateway 9150 unit.

You must have a TFTP server application running on the administration PC. The TFTP server’s base directory must point to the directory that contains the upgrade files.

Manual firmware upgrade

To ensure trouble-free communication between the RLC and Remote Gateway 9150 unit during and after the manual firmware upgrade, Nortel recommends that you perform the upgrades as follows:

- 1 Create backup configuration files for the Remote Gateway 9150 unit and RLC. Refer to “Creating a backup configuration file” on page 282.
- 2 Upgrade the Configuration Manager software on the administration PC.
- 3 Disable the PBX slot(s) where an RLC is installed.
- 4 Upgrade the RLC firmware.
- 5 Upgrade the Remote Gateway 9150 unit firmware.
- 6 Upgrade the BRI module firmware for each BRI module on your Remote Gateway 9150 units.
- 7 Restart the RLC.
- 8 Restart the upgraded Remote Gateway 9150 unit.
- 9 Re-enable the PBX slot(s) where an RLC is installed.

Note: Upgrade the Remote Gateway 9150 unit’s firmware before upgrading the Remote Gateway 9150 unit’s BRI module firmware.

When to perform a firmware upgrade

Perform a firmware upgrade if you have determined that you are using out-of-date firmware. For instructions on determining if you need to perform an upgrade, refer to “Verifying the firmware and software version” on page 335.

ATTENTION!

The protocol for communication between the RLC and the Remote Gateway 9150 units requires that they be running the same version in order for them to communicate with each other.

About firmware upgrades and configuration files

Each time you perform a firmware upgrade, the configuration database is also converted (if necessary) to a format that is compatible with the new firmware. The conversion does not affect configuration settings.

Nortel recommends that each time you perform a firmware upgrade, you first create a backup copy of the converted configuration file and store it in a safe, secure location.

Before you begin

It is important to complete the following steps before performing a firmware upgrade:

- 1 Obtain the firmware upgrade from Nortel.
For instructions, refer to “Obtaining the latest upgrade file” on page 337.
- 2 Extract the upgrade files from the file you received from Nortel.
- 3 Start the TFTP server application.
- 4 Ensure the TFTP base directory reflects the directory where the firmware upgrade file you want to use resides.

Getting there 9150 → Configuration Manager

Upgrading the Remote Gateway 9150 unit firmware

To upgrade the firmware:

- 1 From the Menu Bar, choose Upload/Download → Upload S/W.

Result: The Software Upload dialog box displays, similar to the following:

- 2 Do one of the following:

IF you are upgrading THEN

motherboard firmware, in the Module section, click on the **Application** option button.

ISDN BRI module do the following:

firmware,

- a In the Module section, click on the **BRI** option button.

- b Enter the position on the motherboard where the ISDN BRI module is installed.

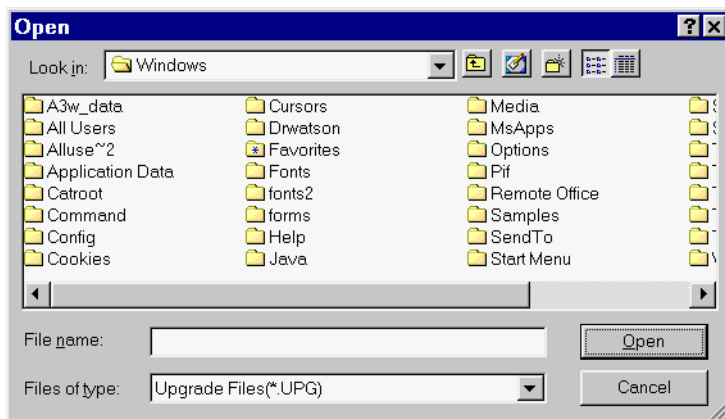
Valid values are 4 through 7.

- 3 Enter the IP address of the TFTP server into the IP Address fields.

Note: Since the TFTP server application runs on your administration PC, this is the IP address of the PC.

- 4 Click on the **Browse** button.

Result: The Open dialog box displays, similar to the following:



- 5 Ensure the Files of type drop down box shows Upgrade Files(*.UPG).
- 6 Navigate to the folder where the firmware file is located.
- 7 Select the file, and then click on the **Open** button.

Examples:

- For motherboard firmware, select 9150-100.upg, and then click on the **Open** button.
- For ISDN BRI module firmware, select briv15u.upg, and then click on the **Open** button.

Result: The Software Upload dialog box re-displays. The file you selected is shown in the Uploaded File field.

- 8 Click on the **Upload** button.

Wait until the file uploads completely before entering any other commands. The Log Report field displays a confirmation message when the upgrade is complete.

- 9 Restart the Remote Gateway 9150 unit.

Automatic or scheduled firmware upgrade

When you configure the Remote Gateway 9150 unit to perform an automatic or scheduled firmware upgrade using the Auto Upgrade Configuration property sheet, the Remote Gateway 9150 unit queries the predefined TFTP server and upgrades the firmware automatically. Refer to “Auto upgrade configuration” on page 243 for further details.



USE CAUTION WHEN FORCING THE AUTO UPGRADE PROCESS AS THE SYSTEM PERFORMS A SELF-RESET ON ALL UNITS TO MAKE THE NEW FIRMWARE ACTIVE ONCE THE DOWNLOAD OF NEW FIRMWARE IS COMPLETE.

Nortel recommends the following when performing an automatic or scheduled firmware upgrade:

- 1 Complete the procedures in “Before you begin” on page 339 prior to configuring the automatic or scheduled upgrade.
- 2 Complete the procedures in “Creating a backup configuration file” on page 282 before performing an automatic or scheduled firmware upgrade.

Notes:

- The automatic or scheduled firmware upgrade only performs upgrades on the Remote Gateway 9100 Series units you configure on the Auto Upgrade Configuration property sheets. In order for the automatic or scheduled firmware upgrade to complete, place the ro-ver.txt file in the same TFTP server directory as you place the .upg file.
- You must perform firmware upgrades on the Remote Gateway 9150 unit's BRI module firmware separately. Refer to “Upgrading the Remote Gateway 9150 unit firmware” on page 340 for further details.

Self-contained firmware upgrade

A self-contained firmware upgrade executable file is also available.

To perform this form of upgrade, both the administration PC and the Remote Gateway 9150 unit must be connected using a 10BaseT Ethernet connection. The self-contained firmware upgrade executable file can run on a Windows 98, NT Workstation 4.0, Millennium Edition (ME), 2000 Professional, or XP (Professional and Home Edition) operating system.

To obtain the self-contained firmware upgrade executable file, click on the **Software Downloads** link at the following website:

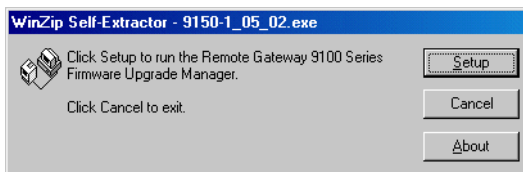
www.nortel.com

Note: You can also email this file to a remote user.

To perform the upgrade:

- 1 Double click on the .exe file.

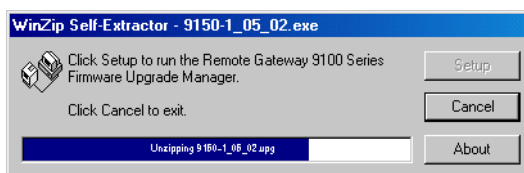
Result: The WinZip Self-Extractor dialog box displays, similar to the following:



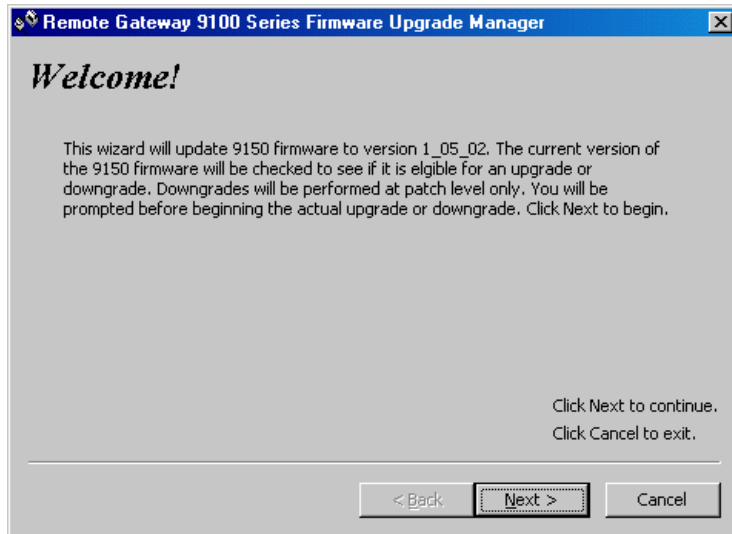
- 2 Click on the **Setup** button to run the Remote Gateway 9100 Series Firmware Upgrade Manager.

Note: You can cancel the upgrade at anytime by clicking on the Cancel button on any of the upcoming dialog boxes. You can find out information regarding this application by clicking on the About button on any of the upcoming dialog boxes.

Result: The WinZip Self-Extractor unzips the Remote Gateway 9150 unit upgrade file and displays an unzip progress bar, similar to the following:

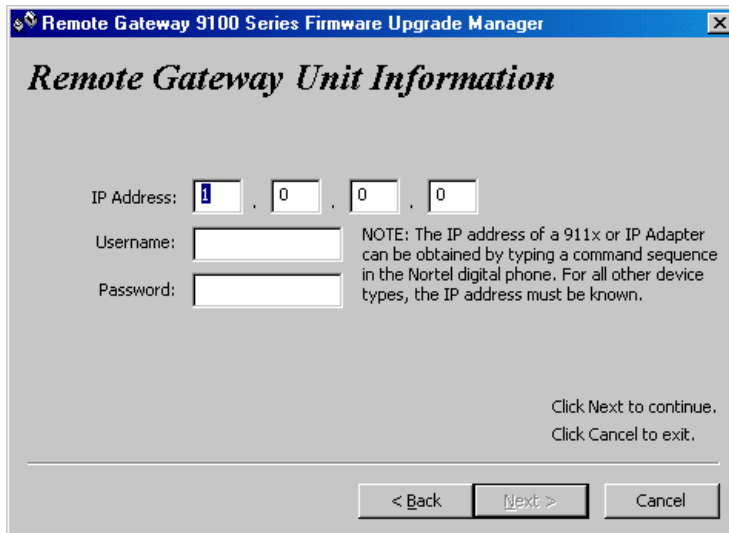


- 3 Once the unzip process is complete, the Welcome dialog box displays, similar to the following:



- 4 Click on the **Next** button.

Result: The Remote Gateway 9100 Series Unit Information dialog box displays, similar to the following:



- 5 Enter the IP address of the Remote Gateway 9150 unit that you want to upgrade.
- 6 Enter your logon name in the Username field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 157 for the default logon ID.
- 7 Enter your password in the Password field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 157 for the default password.
- 8 Click on the **Next** button and follow the instructions on the upcoming dialog boxes to complete the upgrade process.

After successful installation, the executable file removes all residual files excepting the executable itself. For the Remote Gateway 9150 unit, the self-contained firmware upgrade application issues a software-reset command in order to make the new firmware active.

Performing a software upgrade

Perform a software upgrade if you have determined that you are using out-of-date software. For instructions on determining if you need to perform an upgrade, refer to “Verifying the firmware and software version” on page 335.

Upgrading the Configuration Manager software

To upgrade the Configuration Manager software:

- 1 Navigate to the directory that contains the upgrade files you extracted.
- 2 Locate and double-click on the **setup.exe** file.
- 3 Follow the prompts on the screen.

ATTENTION!

Do not ignore any warning messages that the InstallShield displays about versions of files (such as DLL files) that already exist on your PC. If you overwrite these files, you can inadvertently cause other applications on your PC to stop working.

Result: The InstallShield installs the software on top of the previous version.

Chapter 8

Troubleshooting

In this chapter

Before you begin	348
Remote Gateway 9150 unit LED indicators	349
Digital telephone set	351
Device connectivity	356
Software problems	360
Using Configuration Manager PING	362
Syslog testing	365
Alarms and alerts	366
Responding to a catastrophic failure	367
Repair and warranty information	368

Before you begin

If you experience problems in setting up or running your Remote Gateway 9150 unit, this chapter can help you to isolate and solve the problem.

Identifying why a problem occurred

Before you begin, ask yourself the questions listed in the following table:

Question	IF you answered	THEN do the following:
Is this a new installation?	yes	Perform troubleshooting in the sequence presented in this chapter.
	no	Answer the next question.
Did the Remote Gateway 9150 unit work, and then suddenly stop working?	yes	Answer the next question.
	no	Perform troubleshooting in the sequence presented in this chapter.
Did you modify the configuration or change any hardware components?	yes	<ol style="list-style-type: none"> 1 Verify that changes were done correctly. 2 Check the hardware components to ensure they are in working order. 3 Perform troubleshooting for the specific component.
	no	Contact your telecom or data network administrator. There might be a problem with the network.

Remote Gateway 9150 unit LED indicators

During a Remote Gateway 9150 unit power-up cycle, watch the front panel of the Remote Gateway 9150 unit. When the Remote Gateway 9150 unit is functioning properly, the LED indicators do the following:

- The Power LED lights and remains lit.
- The Status LED remains lit after the power-up cycle is completed. The Status LED remains lit all the time when the unit is healthy.
- The remaining LED indicators flash whenever there is network activity.

What to do if the LEDs do not display correctly

The following table describes what to do if the LED indicators do not display correctly:

IF Symptom	THEN What to do
The Status LED indicator is not lit.	1 Did the Status LED indicator ever illuminate? If not, contact your Nortel distributor. There might be a hardware problem.
	2 Are other LED indicators lit or flashing? If no, ensure the power cable is connected to both the power source and the Remote Gateway 9150 unit. If it has become disconnected, reconnect it.
	3 If the Status LED indicator is still out, contact your Nortel distributor. There might be a hardware problem.

IF Symptom	THEN What to do
No LED indicators are lit on the Remote Gateway 9150 unit.	<ol style="list-style-type: none"> 1 Ensure that the Remote Gateway 9150 unit is connected to a power source. 2 If you are using an uninterruptible power supply (UPS), ensure the UPS is powered on. 3 Verify that the AC power source is operational.
The Ethernet COLL LED indicator is lit solid when Half-Duplex Ethernet is enabled in the IP configuration.	<p>Network collisions are bound to occur and are normal. However, if this LED indicator is lit solid when Half-Duplex Ethernet is enabled in the IP configuration, do the following:</p> <ol style="list-style-type: none"> 1 Check the physical network connection. 2 Verify that the Remote Gateway 9150 unit can be PINGed. 3 Check the network configuration (such as routing, traffic load, and so on). Adjust the network configuration, if required. 4 Normally, there is no broadcast or multicast activity on the telephony LAN (TLAN). Interconnect a hub and a network analyzer to the TLAN and monitor for such activity. Identify the source(s) and isolate them from the TLAN.

Digital telephone set

This section identifies some problems that can occur on the digital telephone set, and describes what to do to resolve them.

Symptoms descriptions

If you are having trouble with digital telephones, perform troubleshooting as described in the following table:

Symptom	What to do
There is no dial tone when pressing either the host call appearance or local call appearance keys.	<ol style="list-style-type: none">1 Is this a first-time installation? If yes, perform troubleshooting as described in “What to do if the telephone connection tests do not work” on page 130.2 If you are trying to place a host-controlled call, check the IP network and ensure that<ul style="list-style-type: none">■ it is not down■ traffic is being routed between the Remote Gateway 9150 unit and RLC on the host PBX3 If you are trying to place a host- or locally controlled call, Ensure the ISDN BRI line is working. Ask your service provider to check this.4 Restart the RLC, wait one minute, and then restart the Remote Gateway 9150 unit.5 Ensure the RLC is enabled in its host PBX slot. In Load 97 on the Meridian 1 PBX, stat the RLC, disable and enable it, or re-seat it if necessary.

Symptom	What to do
There is no dial tone when pressing either the host call appearance or local call appearance keys. (continued)	6 Contact your telecom administrator. There might be problems at the host PBX.
A stutter is heard during a remote dial tone.	<p>This is a normal occurrence and is caused by the DSP activating a dial tone relay. However, to eliminate stutter dial tone, disable Dialtone Relay. Dialtone Relay settings are in the Advanced Configuration dialog box, which is available on the RLC System Configuration Property sheet.</p>
Lamps or indicators are not lit after completion of a Remote Gateway 9150 unit power cycle.	<ol style="list-style-type: none"> 1 Check all cable connections to and from the Remote Gateway 9150 unit and ensure they are all securely connected. 2 Is this a first-time installation? If yes, check the telephone connections. Refer to the Telco 1 and Telco 2 cable pin-out tables in Appendix C, "Pin-out tables for connections." 3 Ensure the ISDN BRI line is working. Ask your service provider to check this. 4 Check the IP network and ensure that: <ul style="list-style-type: none"> ■ it is not down ■ traffic is being routed between the Remote Gateway 9150 unit and RLC on the host PBX 5 PING the RLC from the Remote Gateway 9150 unit to verify IP network connectivity.
Lamps or indicators do not reflect the true status of the telephone.	<p>It is possible that there is a synchronization error between the Remote Gateway 9150 unit and the host PBX. Contact your telecom network administrator.</p>

Symptom	What to do
The display is blank (that is, the time and date are not displayed).	<ol style="list-style-type: none">1 Take the digital telephone handset off hook and dial the Online SPRE code. The Remote Gateway 9150 unit attempts to connect to the host PBX. When the connection is established, the time and date display.2 Check the IP network and ensure that:<ul style="list-style-type: none">■ it is not down■ traffic is being routed between the Remote Gateway 9150 unit and RLC on the host PBX3 PING the RLC from the Remote Gateway 9150 unit to verify IP network connectivity.4 Ensure the ISDN BRI line is working. Ask your service provider to check this.5 Restart the RLC, wait one minute, and then restart the Remote Gateway 9150 unit.6 Ensure the RLC is enabled in its host PBX slot.<p>In Load 97 on the Meridian 1 PBX, stat the RLC, disable and enable it, or re-seat it if necessary.</p>7 Contact your telecom administrator. There might be problems at the host PBX.

Symptom	What to do
There are noticeable gaps or poor quality when a voice call is active on the IP network.	<ol style="list-style-type: none"> 1 Check the Quality of Service (QoS) configuration on the RLC. Adjust the configuration, if required. Lower the QoS threshold so that transition occurs earlier. 2 Analyze the traffic patterns on your voice and IP networks as described in the <i>Remote Gateway 9100 Series Network Engineering Guidelines</i> (555-8421-230). It is possible that your IP network capacity cannot accommodate the additional voice data, especially during High Day Busy Hour (HDBH) periods. Make adjustments to your network as required.
Incoming calls are not being received from the host PBX.	<ol style="list-style-type: none"> 1 Ensure your telephone is not on call forward. 2 Ensure the Remote Gateway 9150 unit is not in offline mode by entering the Online SPRE code at a digital telephone. 3 Ensure the Remote Gateway 9150 unit is powered up. It cannot receive calls from the host PBX if it is not powered up. 4 Ensure the RLC is correctly configured with your Remote Gateway 9150 unit's IP address, telephone number, and security ID (if they are used). 5 Ensure the ISDN BRI line is working, if it is being used to route host-controlled calls. Ask your service provider to check this.

Symptom	What to do
Incoming calls are not being received from the host PBX. (continued)	<p>6 Check the IP network (if it is being used) and ensure that:</p> <ul style="list-style-type: none"> ■ it is not down ■ traffic is being routed between the Remote Gateway 9150 unit and RLC on the host PBX <p>7 PING the RLC from the Remote Gateway 9150 unit to verify IP network connectivity.</p> <p>8 If the problem persists, contact your telecom administrator or Nortel distributor.</p>
Incoming calls are not being received from the PSTN.	<p>1 Ensure your telephone is not on call forward.</p> <p>2 Ensure the calling party has your office's correct telephone number.</p> <p>3 Ensure the Remote Gateway 9150 unit is powered up. It cannot receive calls from the host PBX or the PSTN if it is not powered up.</p> <p>4 Ensure the ISDN BRI line is working. Ask your service provider to check this.</p> <p>5 If the problem persists, contact your telecom administrator or Nortel distributor.</p>
A call in progress was suddenly disconnected.	<p>1 Does your telephone display "Offline Mode?" If so, enter the Online SPRE code to go back online.</p> <p>2 Contact your telecom and data network administrators. Perhaps network problems caused the call to drop.</p>

Device connectivity

This section identifies some problems that can occur on the data network, and describes what to do to resolve them.

Symptom descriptions

If you are not able to establish or maintain data network connectivity, perform troubleshooting as described in the following table.

Note: To enable valid loopback testing of serial ports and cables, Nortel recommends that you use a breakout box.

Symptom	What to do
SERIAL CONNECTION FAILED displays when attempting to connect to the Remote Gateway 9150 unit.	<ol style="list-style-type: none"> 1 Ensure that you entered the logon ID and password correctly when trying to establish the connection. 2 Ensure that someone else is not already logged on to the Remote Gateway 9150 unit. 3 Ensure that you selected the correct COM port when trying to establish the connection. 4 Verify that no other applications on the administration PC are using the COM port. 5 Verify that the serial connection is good. 6 Using a breakout box, verify that the COM port is active. 7 Ensure the Remote Gateway 9150 unit is powered up. 8 Power the Remote Gateway 9150 unit off, and then back on. 9 Contact your Nortel distributor. There might be a hardware problem.

Symptom	What to do
10060 TELNET CONNECTION FAILED displays when attempting to connect to the Remote Gateway 9150 unit.	<ol style="list-style-type: none">1 Ensure that you entered the logon ID and password correctly when trying to establish the connection.2 Ensure that you entered the IP address correctly when trying to establish the connection.3 Ensure that someone else is not already logged on to the Remote Gateway 9150 unit.4 Verify that the Ethernet cable is connected at both ends (the Remote Gateway 9150 unit and the network hub).5 Check the Ethernet cable and ensure it is good.6 Ensure the Remote Gateway 9150 unit is powered up.7 Power the Remote Gateway 9150 unit off, and then back on.8 Ensure the Remote Gateway 9150 unit's IP address, network mask, and default gateway are correctly configured in the Remote Gateway 9150 unit.9 PING the Remote Gateway 9150 unit to see if it responds.10 If the Remote Gateway 9150 unit does not respond, PING the Remote Gateway 9150 unit's gateway to see if it responds.11 If the gateway does not respond, PING a known good device on the Remote Gateway 9150 unit's network.12 If steps 10 and 11 work, but step 9 did not, there might be a gateway configuration error. Contact your data network administrator.13 Contact your Nortel distributor. There might be a hardware problem.

Symptom	What to do
There are many collisions on the Ethernet network, as indicated by a solid Ethernet COLL LED indicator when the Remote Gateway 9150 unit is configured for half-duplex Ethernet traffic.	<p>Network collisions are bound to occur and are normal. However, if this LED indicator is lit solid, do the following:</p> <ol style="list-style-type: none"> 1 Check the physical network connection. 2 Verify that the Remote Gateway 9150 unit can be pinged. 3 Check the network configuration (such as routing, traffic load, and so on). Adjust the network configuration, if required. 4 Normally there is no broadcast or multicast activity on the TLAN. Interconnect a hub and a network analyzer to the TLAN and monitor for such activity. Identify the source(s) and isolate them from the TLAN.
The Remote Gateway 9150 unit will not send or receive Ethernet traffic.	<ol style="list-style-type: none"> 1 Ensure that the Remote Gateway 9150 unit is powered up. The Remote Gateway 9150 unit cannot send or receive traffic if it is not powered up. 2 Check the Ethernet cable between the Remote Gateway 9150 unit and the network, and ensure that it is good. 3 Ensure the Ethernet cable is connected. 4 If the Remote Gateway 9150 unit still will not send or receive traffic, contact your data network administrator. 5 Data network administrator: Ensure that other network devices are configured to allow traffic to and from the Remote Gateway 9150 unit.
An attempt to log off from the Remote Gateway 9150 unit does not work.	<p>It is possible that communication has been lost between the administration PC and the Remote Gateway 9150 unit.</p> <p>Close Configuration Manager, and then restart it.</p>

Symptom	What to do
The Remote Gateway 9150 unit cannot establish a connection with the RLC.	<ol style="list-style-type: none">1 Verify security authentication configuration and ensure that it matches at both ends. (For example, if the security identifier security level is used, ensure that the inbound and outbound security identifiers are correctly configured at each end.)2 Ensure that the unit IDs have been correctly configured at each end. An incorrect unit ID causes security authentication to fail.3 Ensure that the RLC's IP address and PSTN number are correctly configured on the Remote Gateway 9150 unit (as appropriate).4 Verify that the IP network and PSTN are operational (up and running) as appropriate.5 Ensure that the RLC is enabled on the host PBX.6 Use the Ping option in Configuration Manager to PING the RLC. For instructions, refer to "Using Configuration Manager PING" on page 362.7 If the RLC does not respond, check the network configuration (such as, routing, traffic load, and so on). Adjust the network configuration, if required.

Software problems

This section identifies some problems that can occur with the Configuration Manager software, and describes what to do to resolve them.

Symptom descriptions

If you are not able to complete a task with Configuration Manager, perform troubleshooting as described in the following table:

Symptom	What to do
The Configuration Manager software installation fails.	Ensure that you close all background applications, including anti-virus checking software before performing the installation.
When performing one of the following by TFTP, <code>ERROR: FILE OPEN FAILED</code> displays: <ul style="list-style-type: none">■ configuration upload■ firmware upgrade	<ol style="list-style-type: none">1 Ensure the TFTP server application is installed and running on your administration PC.2 Ensure the file you are trying to upload is present in the target directory. That is, either in the TFTP directory, or in the directory that is specified as the base directory in the TFTP server application.3 Review messages displayed by the TFTP server application for clues.4 PING the Remote Gateway 9150 unit to verify that network connectivity exists.
<code>CONFIG UPLOAD FAILED</code> when attempting to perform a configuration upload by TFTP.	<ol style="list-style-type: none">1 Ensure that you selected an appropriate file. That is, ensure that the file you attempted to upload is a Remote Gateway 9150 configuration file.

Symptom	What to do
<p>CONFIG UPLOAD FAILED when attempting to perform a configuration upload by TFTP. (continued)</p>	<p>2 Ensure that the configuration file you are attempting to upload is compatible with current Remote Gateway 9150 firmware. Perform the configuration upload using a previous configuration file, if necessary.</p> <p>Note: Each time you perform a Remote Gateway 9150 firmware upgrade, create a backup of the configuration. The configuration database format in the Remote Gateway 9150 unit is dependent on the version of firmware installed on the Remote Gateway 9150 unit. If you recently downgraded to a previous version of Remote Gateway 9150 firmware, you might also need to revert to a previous configuration format.</p>
<p>System not responding displays when working with Configuration Manager.</p>	<p>It is possible that communication has been lost between the administration PC and the Remote Gateway 9150 unit.</p> <p>Close Configuration Manager, and then restart it.</p>
<p>Nothing happens when attempting to log off from the Remote Gateway 9150 unit.</p>	<p>It is possible that communication has been lost between the administration PC and the node you were logged on to.</p> <p>Close Configuration Manager, and then restart it.</p>

Using Configuration Manager PING

PING, or Packet InterNet Groper, is a protocol and program to test whether a device is accessible on a network. This section explains how to use the PING option provided in Configuration Manager to verify network connectivity. Use this procedure as a troubleshooting tool to determine if you can reach the RLC, another remote unit, or any other device on the network.

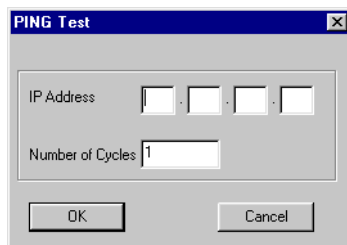
Getting there 9150 → Configuration Manager

Performing a Configuration Manager PING

To perform a Configuration Manager PING:

- 1 From the Menu Bar, choose Tests → Ping.

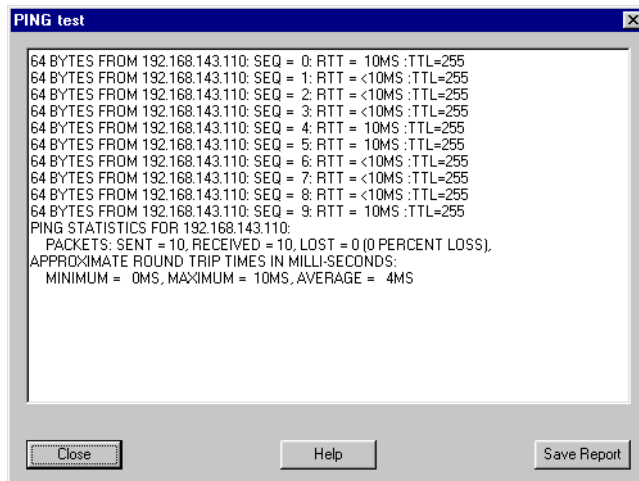
Result: The PING Test dialog box displays, similar to the following:



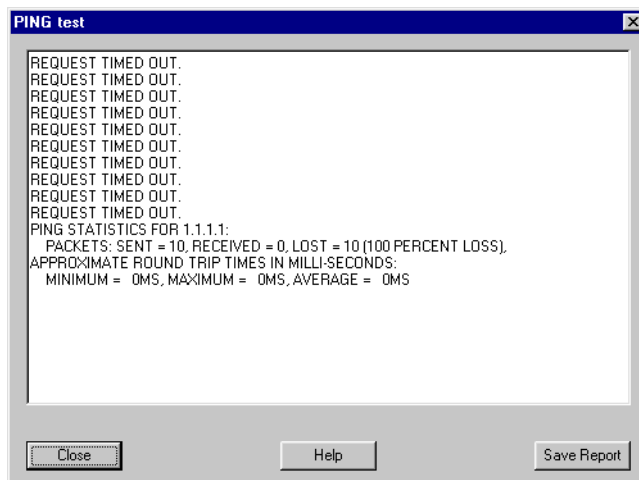
- 2 Enter the IP Address of the unit you want to PING in the IP Address field.
- 3 Enter the number of times you want to PING the unit in the Number of Cycles field (1 to 100).

- 4 Click on the **OK** button.

Result: The PING test window displays, showing the PING results. The following is an example of a successful PING:



The following is an example of an unsuccessful PING:



- 5 Click on the **Close** button.

Result: The PING test window closes.

ATTENTION!

It is possible to successfully PING a device on the network and still not be able to log on to that device. If you log on to a device (a Remote Gateway 9150 unit) using a serial connection and neglect to log off, you may be able to successfully PING the device but be unable to establish a Telnet connection to it. (The device believes itself to be busy.)

If you cannot log on to a device after a successful PING, access the serial port and ensure that you are not logged on to the device through this port.

Unsuccessful PING options

If the PING was unsuccessful:

- 1** Ensure you have entered the IP address, subnet mask, and default gateway correctly.
- 2** PING the gateway to see if it responds.
- 3** Contact your data network administrator if the PING still does not work.

Syslog testing

Once you configure the syslog feature and save it to Flash, use the Syslog test command to test the configuration. The 9150 system generates test syslog messages. This allows you to verify the syslog configuration as well as the syslog collector functionality on the syslog server(s).

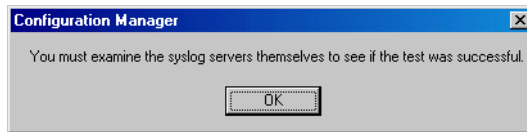
Getting there 9150 → Configuration Manager

Performing Syslog testing

To perform syslog testing:

- 1 From the Menu Bar, choose Tests → Syslog.

Result: A message displays, similar to the following:



- 2 Click on the **OK** button.
- 3 Examine the syslog server(s) to see if the test was successful.

Alarms and alerts

For troubleshooting purposes, each Remote Gateway 9100 Series device transmits alarms and alerts to the host PBX. These alarms and alerts indicate to the host PBX that the Remote Gateway 9100 Series device is in a state of alarm or alert. The host PBX then produces an alarm or alert through its software. Refer to “Display logs” on page 412 to determine if the host PBX produces an alarm or alert when Remote Gateway 9100 Series Configuration Manager produces a display log.

Responding to a catastrophic failure

For the purposes of this discussion, a *catastrophic failure* is defined as a failure of the equipment to operate after review of all troubleshooting information and implementation of appropriate procedures.

Inoperative hardware

If your RLC fails to operate after thorough review of the troubleshooting information in this and related Guides, consult your Nortel distributor for hardware replacement.

Repair and warranty information

The Remote Gateway 9150 unit contains no user-serviceable components. If the problem experienced with your Remote Gateway 9150 unit persists after you have used all the appropriate procedures in this chapter, refer to the following contact information for repair and warranty help, depending upon your location.

Note: If the Remote Gateway 9150 unit is causing harm to the telephone network, the telephone company may request that you disconnect it pending resolution of the problem.

Canada

Nortel Service Selection Center
30 Norelco Drive
Weston, ON
Canada

M9L 2X6

Telephone: 1-800-466-7835

United States

Nortel
Product Service Center
640 Massman Drive
Nashville, TN 37210
USA

Telephone: 1-800-466-7835

Europe

Nortel (NI) Ltd.
FAO: Irish Express Cargo (IEC)
Raheen Industrial Estate
Raheen, Limerick
Ireland

Telephone: 00 800 8008 9009 or +44 (0) 870 907 9009
Fax: +33 4 9296 1598

Asia/Pacific

Nortel Distribution Center
c/o ACCO Transport
21 South St. Unit#2
Rydalmere, NSW
2116 Australia

CALA

Note: When you need warranty and repair service in Central American and Latin American countries, you must first get an RR (repair and return) number from your Nortel distributor before shipping to the Nortel CALA Repair Center.

Nortel c/o Wesbell
4019 S.W. 30th Avenue
Fort Lauderdale, FL 33312
USA
Notify: Receiving Department
RR no.:

Telephone:
Normal Service Hours (Monday through Friday, 8:00 a.m. to 5:00 p.m. Central Time): 1-954-851-8841
After Normal Hours (weekends and holidays): 1-888-594-8474

Fax: 1-954-581-2334

Appendix A

Planning forms

In this appendix

Overview	372
Completing the Remote Gateway 9150 forms	374
Configuration Information—Stations	376
Configuration Information—ISDN BRI Modules	380
Configuration Information—Network Connections	383
Configuration Information—Dialing Plans	384
System expansion worksheet	385

Overview

This appendix provides several forms that you can use to plan and record the various data necessary for proper configuration of a Remote Gateway 9150 unit at your site.

Note: RLC forms are provided in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Network planning

To help you plan your Remote Gateway 9100 Series network, study the network diagram and sample configurations provided in Appendix B, “Sample configuration files.” The information provided in this appendix demonstrates the relationships between RLC and Remote Gateway 9150 configuration settings.

Remote Gateway 9150 forms

Use the Remote Gateway 9150 forms to record information and calculate needed resources for a Remote Gateway 9150 unit. For more information about using these forms, refer to “Planning the configuration” on page 81.

Data entry form completion sequence

Information from some forms might need to be copied to other forms. Nortel recommends that you complete the data entry forms in the following sequence:

1. Remote Gateway 9150 Configuration Information—Stations form
2. Reach Line Card Connection Information (for either the 16-port or 32-port RLC)
3. Remote Gateway 9150 Configuration Information—Network Connections form

4. Remote Gateway 9150 Configuration Information—ISDN BRI Modules form
5. Remote Gateway 9150 Configuration Information—Dialing Plans form
6. Reach Line Card Online/Offline Table Configuration (if required)

For more details, refer to “Completing the Remote Gateway 9150 forms” on page 374.

Completing the Remote Gateway 9150 forms

This section briefly describes how to complete the Remote Gateway 9150 configuration forms.

To complete the forms:

- 1 Assign each user telephone or fax machine to a port on the Remote Gateway 9150 unit.

Record the assignments on the Remote Gateway 9150 Configuration Information—Stations form. Designate each port as a local port, remote port, or local and remote port.
- 2 Use the information you received from the ISDN service provider for the Remote Gateway 9150 site to complete the Remote Gateway 9150 Configuration Information—ISDN BRI Modules form.

At the same time, do the following:

- a. Designate a B-channel as a primary trunk. The Remote Gateway 9150 unit uses primary trunk to establish connections between the Remote Gateway 9150 unit and the RLC.

Note: The primary trunk on the Remote Gateway 9150 unit is defined as follows:

- the lowest-numbered B-channel defined as Remote only
- the lowest-numbered B-channel defined as Local and Remote

Do not include the primary trunk in any trunk groups. Nortel recommends that you define the primary trunk as Remote only.

Record the primary trunk assignment in the “Connection to RLC information” section on the Remote Gateway 9150 Configuration Information—Network Connections form.

- b. Assign B-channels to trunk groups. Record the assignments on the ISDN BRI Modules form.

- 3 Assign an IP address, subnet mask, and gateway to the Remote Gateway 9150 unit. This information is required if you want to administer the Remote Gateway 9150 unit over the IP network.

Record the addresses in the “Remote Gateway 9150 unit identification” section on the Remote Gateway 9150 Configuration Information—Network Connections form.

- 4 If the security level chosen is security code, record the security identifier assigned to the Remote Gateway 9150 unit.
- 5 In the “Connection to RLC information” section on the Remote Gateway 9150 Configuration Information—Network Connections form, record the RLC’s

- IP address
- telephone number
- security code

The Remote Gateway 9150 unit uses this information to establish and authenticate connections with the RLC.

- 6 If an online/offline table is configured on the RLC, configure the SPRE codes for toggling the online/offline modes on the Remote Gateway 9150 unit.

Note: This step is optional, because default SPRE codes have already been defined in the software (as indicated on the Remote Gateway 9150 Configuration Information—Dialing Plans form).

If you choose to change the code, record the new code on the Dialing Plans form.

- 7 Define the trunk access and Paging SPRE codes.

Trunk access codes are used by Remote Gateway 9150 unit users to get outside lines.

Note: Default trunk access digits and paging SPRE codes have already been defined. Nortel recommends that you use the defaults.

If you choose to change the predefined codes, record them on the Remote Gateway 9150 Configuration Information—Dialing Plans form. Also, record the trunk access codes (as required) on the ISDN BRI Modules form.

Remote Gateway 9150

Configuration Information—Stations

Page 1 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
0		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
1		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
2		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
3		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
4		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
5		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
6		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
7		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
8		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
9		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
10		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
11		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
12		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
13		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
14		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
15		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
16		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
17		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
18		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No

Remote Gateway 9150

Configuration Information—Stations

Page 2 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
19		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
20		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
21		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
22		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
23		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
24		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
25		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
26		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
27		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
28		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
29		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
30		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
31		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No

Use ports 32 through 63 only if this Remote Gateway 9150 unit connects to a 2-slot RLC on the host PBX.

32		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
33		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
34		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
35		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No

Remote Gateway 9150

Configuration Information—Stations

Page 3 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
36		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
37		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
38		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
39		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
40		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
41		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
42		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
43		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
44		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
45		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
46		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
47		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
48		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
49		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
50		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
51		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
52		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
53		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No

Remote Gateway 9150

Configuration Information—Stations

Page 4 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
54		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
55		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
56		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
57		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
58		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
59		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
60		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
61		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
62		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
63		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No
64: FAX		<input type="checkbox"/> Local	<input type="checkbox"/> Remote	<input type="checkbox"/> Both		<input type="checkbox"/> Yes	<input type="checkbox"/> No

Remote Gateway 9150

Configuration Information—ISDN BRI Modules

Page 1 of 3

Module 4

ISDN line type (variant): _____	Switch type: _____
B-channel 1 DN: _____	SPID: _____
	Connection type: <input type="checkbox"/> Local <input type="checkbox"/> Local and Remote <input type="checkbox"/> Remote
Trunk group: _____	Trunk access code: _____
B-channel 2 DN: _____	SPID: _____
	Connection type: <input type="checkbox"/> Local <input type="checkbox"/> Local and Remote <input type="checkbox"/> Remote
Trunk group: _____	Trunk access code: _____

Module 5

ISDN line type (variant): _____	Switch type: _____
B-channel 1 DN: _____	SPID: _____
	Connection type: <input type="checkbox"/> Local <input type="checkbox"/> Local and Remote <input type="checkbox"/> Remote
Trunk group: _____	Trunk access code: _____

Remote Gateway 9150

Configuration Information—ISDN BRI Modules

Page 2 of 3

Module 5 (continued)

B-channel 2 DN:	SPID:
_____	_____
	Connection type:
	<input type="checkbox"/> Local <input type="checkbox"/> Local and Remote
	<input type="checkbox"/> Remote
Trunk group:	Trunk access code:
_____	_____

Module 6

ISDN line type (variant):	Switch type:
_____	_____
B-channel 1 DN:	SPID:
_____	_____
	Connection type:
	<input type="checkbox"/> Local <input type="checkbox"/> Local and Remote
	<input type="checkbox"/> Remote
Trunk group:	Trunk access code:
_____	_____
B-channel 2 DN:	SPID:
_____	_____
	Connection type:
	<input type="checkbox"/> Local <input type="checkbox"/> Local and Remote
	<input type="checkbox"/> Remote
Trunk group:	Trunk access code:
_____	_____

Remote Gateway 9150

Configuration Information—ISDN BRI Modules

Page 3 of 3

Module 7

ISDN line type (variant): _____	Switch type: _____
B-channel 1 DN: _____	SPID: _____
	Connection type: <input type="checkbox"/> Local <input type="checkbox"/> Local and Remote <input type="checkbox"/> Remote
Trunk group: _____	Trunk access code: _____
B-channel 2 DN: _____	SPID: _____
	Connection type: <input type="checkbox"/> Local <input type="checkbox"/> Local and Remote <input type="checkbox"/> Remote
Trunk group: _____	Trunk access code: _____

Remote Gateway 9150

Configuration Information—Network Connections

Page 1 of 1

Security level:		<input type="checkbox"/> No security	<input type="checkbox"/> Caller ID	<input type="checkbox"/> Provision ID
Remote Gateway 9150 unit identification				
Node number:	_____		Node name:	_____
IP address:	<div style="display: flex; justify-content: space-between;"> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> </div>			
Subnet mask:	<div style="display: flex; justify-content: space-between;"> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> </div>			
Default gateway:	<div style="display: flex; justify-content: space-between;"> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> </div>			
If the security level is Provision ID, what is the Remote Gateway 9150 unit's security identifier?				

Connection to RLC information				
IP address to reach the host PBX (for IP network):				
<div style="display: flex; justify-content: space-between;"> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> <div><div style="border: 1px solid black; width: 20px; height: 20px;"></div></div> </div>				
Telephone number to reach host PBX (for PSTN): _____				
If security level is Provision ID, what is the RLC's security identifier? _____				
Trunk dedicated as the primary trunk:				
Note: Refer to the Remote Gateway 9150 Configuration Information—ISDN BRI Modules form.				
Module:	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
B-channel	<input type="checkbox"/> 1	<input type="checkbox"/> 2		

Remote Gateway 9150

Configuration Information—Dialing Plans

Page 1 of 1

Notes:

- Nortel recommends that you use the pre-configured default codes listed below.
- The pound sign (# in North America) is mandatory and is automatically pre-configured in Configuration Manager. The pound sign prevents conflicts with the dialing plan on the host PBX.
- You can dedicate all B-channels to one trunk group. You do not have to create a trunk group for each B-channel.

Description	Default code	Your code (maximum of 3 digits)
Online SPRE code	#99	#
Offline SPRE code	#98	#
Paging SPRE code	#05	#
Local Calling SPRE code (for analog or ATA-equipped stations)	#8	#
Registration SPRE code (for multi-user or dynamic pool ports only)	#97	#
De-registration SPRE code (for multi-user or dynamic pool ports only)	#96	#
Access code for trunk group 1	#61	#
Access code for trunk group 2	#62	#
Access code for trunk group 3	#63	#
Access code for trunk group 4	#64	#
Access code for trunk group 5	#65	#
Access code for trunk group 6	#66	#
Access code for trunk group 7	#67	#
Access code for trunk group 8	#68	#

Remote Gateway 9150

System expansion worksheet

Page 1 of 4

Complete one worksheet for each Remote Gateway 9150 unit.

Number of simultaneous fax calls

- 1 How many simultaneous faxes do you want your equipment to support?

Multiply the number of simultaneous faxes by two to determine the total number of DSP channels required for fax calls. (Each fax call requires two DSP channels.)

_____ x 2 = _____

Notes:

- If the number of DSP channels required for fax calls is not divisible by four, round up the number entered in step 1 to the next multiple of four. (Each DSP device contains four channels.)
- Always round up to a higher number.

- 2 Divide your Step 1 answer, the total number of DSP channels required for fax calls, by four to determine the number of DSP devices required for fax calls. (Configuration Manager assigns DSP function on a per-device basis.)

Step 1: _____ / 4 = _____

Note: This calculation assumes G.729A/FAX compression. For G.711 or G.726, divide by four.

Number of stations:

- 3 How many digital telephones will be installed at the Remote Gateway 9150 site?

Note: A maximum of 32 digital telephones can be connected to the Remote Gateway 9150 unit.

- 4 How many Analog Telephone Adapters (ATAs) will be installed?

- 5 How many Meridian Communication Adapters (MCAs) will be installed?

- 6 Add lines 3 and 4 together.

Notes:

- A maximum of four MCAs and ATAs can be installed when connecting the Remote Gateway 9150 unit to a 1-slot RLC. A maximum of seven MCAs and ATAs can be installed when connecting to a 2-slot RLC.
- The total number of ATAs and digital telephones cannot exceed 32.

- 7 Will a fax machine be used for faxes through the host PBX? ☐ Yes

☐ No

- 8 If line 7 is Yes, add 2 to line 6.

Remote Gateway 9150

System expansion worksheet

Page 2 of 4

Call blocking:

- 9 Do you want to implement call blocking? (Users will receive a fast busy signal when resources are not available.) ☐ Yes ☐ No

- 10 If line 9 is Yes, calculate the number of calls that can be active at one time.
Note: A conservative estimate of one call in three being blocked when no resources are available is recommended.
Multiply line 6 by your call blocking factor. For example, to calculate the number of simultaneous calls that can be supported at a 3:2 blocking ratio, multiply line 8 by 2/3 (0.666). If the result contains a fraction, round up to a whole number.

Line 8: _____ x _____ = _____

If line 9 is No, the number of simultaneous calls is the same as the number of stations installed. (Record your response to line 8 here.) _____

Call routing:

- 11 How do you want to route host-controlled calls?

☐ IP network ☐ PSTN ☐ Both

Note: If you want to route host-controlled calls over both networks, then you can use QoS Transitioning Technology.

- 12 If line 11 is PSTN or Both, do you want to support locally controlled calls through the PSTN (that is, support local calling)? ☐ Yes ☐ No

Number of trunk interface modules needed for QoS transition support or routing calls over the PSTN

Note: If you are routing calls over the IP network only, skip this section.

- 13 If line 12 is No, enter 0.

If line 12 is Yes, how many simultaneous digital telephone or ATA local calls do you want to support?

Enter a value between 1–7.

Note: Only one active call per ISDN BRI B-channel is allowed in locally controlled mode because local calls are not compressed. _____

Remote Gateway 9150

System expansion worksheet

Page 3 of 4

Number of trunk interface modules needed (continued):

- 14 Calculate the number of B-channels required for simultaneous calls in host-controlled mode.

Each B-channel can support one MCA call, or up to eight simultaneous voice calls using G.729A compression (where each call is compressed to 8 Kbps). However, when using G.729A compression, the first B-channel can support only six simultaneous calls because 16 Kbps are required for transporting call signaling data for the entire Remote Gateway 9150 unit (and all of its connected stations) to the host PBX.

Line 5: _____ + ((# of simultaneous calls: _____ * 8 Kbps) + 16 Kbps) / 64 = _____

Round up the result to a whole number. _____

- 15 Calculate the number of B-channels required for both locally controlled and host-controlled calls. Add lines 13 and 14. _____

If the result is greater than 8, then call blocking must be implemented, or the number of simultaneous local calls must be reduced.

Recalculate lines 10, 13, 14, and 15. _____

- 16 Calculate the number of trunk interface modules required for local calls. Divide line 15 by 2. If the result contains a fraction, round it up to the next whole number.

Line 15: _____ / 2 = _____

- 17 How many trunk interface modules are already installed in the Remote Gateway 9150 unit? _____

- 18 Calculate the number of trunk interface modules you need to purchase. Subtract line 17 from line 16. _____

Note: A maximum of four trunk interface modules can be installed in the Remote Gateway 9150 unit.

Remote Gateway 9150
System expansion worksheet

Page 4 of 4

Number of DSP application modules needed:	
19	<p>Each DSP application module can support up to eight simultaneous calls over the IP network.</p> <p>Add line two to line eight, divide the sum by eight, and round up to the next whole number.</p> <p>(Line 2: _____ + Line 10: _____) / 8 = _____</p>
20	<p>Record the number of DSP application modules already installed.</p> <p>Note: The Remote Gateway 9150 unit ships from Nortel with the equivalent of two DSP application modules built in. Your response here must include those modules.</p> <p>_____</p>
21	<p>Calculate how many DSP modules you need to purchase.</p> <p>Subtract line 20 from line 19.</p> <p>Note: A maximum of three DSP application modules can be installed in the Remote Gateway 9150 unit.</p> <p>_____</p>

Appendix B

Sample configuration files

In this appendix

Example of a network	390
Voice port configuration on the Meridian 1 PBX	392
Data port configuration on the Meridian 1 PBX	394
RLC configuration	396
Remote Gateway 9150 unit configuration	400

Example of a network

This section provides an example of a network diagram that shows one host site (with one RLC installed on the host PBX) and one Remote Gateway 9150 unit (with one user station). The purpose of this diagram is to demonstrate the relationship between configuration settings on each unit in the network.

Sample configuration printouts

Sample Meridian 1 PBX configuration printouts for the voice and data ports are provided as follows:

- voice port: on page 392
- data port: on page 394

Sample configuration printouts for the RLC and Remote Gateway 9150 unit are shown as follows:

- RLC: on page 396
- Remote Gateway 9150 unit: on page 400

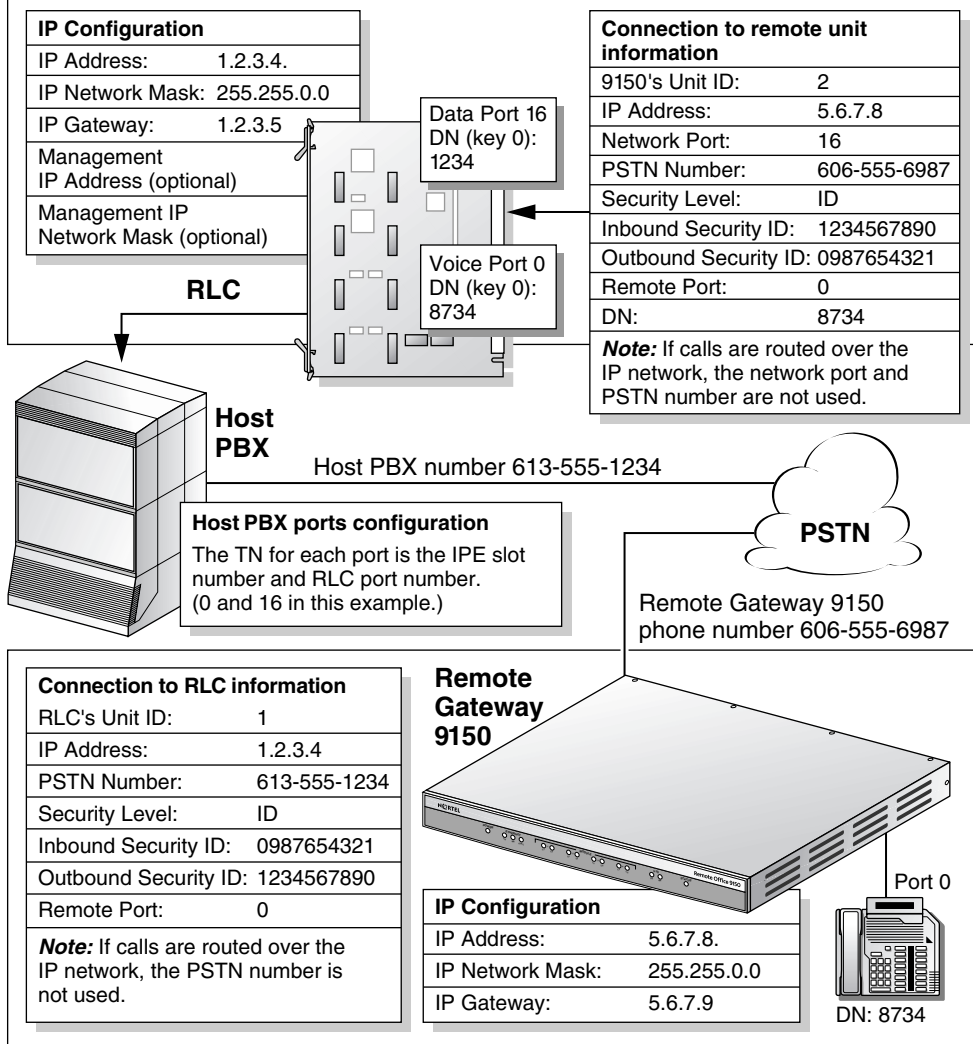
Configuration recommendation

The quickest way to configure the RLC and Remote Gateway 9150 unit is to run the Configuration Wizard. For instructions, refer to “Using the Configuration Wizard to perform initial configuration” on page 115. For your reference, the Configuration Wizard screen examples are completed using the same information.

Note: The network diagram shows information that cannot be configured through the Configuration Wizard, such as the security identifiers. You must use Configuration Manager to complete the configuration.

Network diagram

Note: This diagram assumes that both the IP and PSTN are being used.



G101413

Voice port configuration on the Meridian 1 PBX

This section shows the configuration settings for the voice port on the Meridian 1 PBX. Generally, define voice ports according to the needs of your remote users.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 391.

Note: This configuration example is from a Meridian 1 PBX 11.

```
REQ: prt
TYPE: 2616
MARP NOT ACTIVATED
TN 5 0
DATE
PAGE
DES
DES Bryan Dion
TN 005 0 00 00
TYPE 2616
CDEN 8D
CUST 0
AOM 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
```

← Telephone type

← RLC slot and port numbers

```

CLS   CTD FBD WTA LPR MTD FND HTD ADD HFD
      MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
      POD DSX VMD CMSD CCSD SWD LND CNDD
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
      ICDD CDMD LLCN MCTD CLBD AUTU
      GPUD DPUD DNDD CFXD ARHD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AHD
      DDGA NAMA
      DRDD EXR0
      USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3
CPND LANG ENG
HUNT
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU LANG 0
DNDR 0
KEY 00 SCR 8734 0      MARP
      CPND
      NAME Bryan Dion
      XPLN 24
      DISPLAY_FMT FIRST, LAST
01 CWT
02 MSB
03 TRN
04 CFW 4
05 AO6
06
07
08
09
10 MCR 8234 0 MARP
      CPND
      NAME Bryan Dion
      XPLN 24
      DISPLAY_FMT FIRST, LAST
11 AO6
12
13 DSP
14
15

```

← VCE defines the port as a voice port.

← 9150 unit user's DN

← 9150 unit user's CPND

Data port configuration on the Meridian 1 PBX

This section shows the configuration settings for the data port on the Meridian 1 PBX. The data port provides the communication path between the RLC and the Remote Gateway 9150 unit, and must be configured as an MCA.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 391.

Note: This configuration sample is from a Meridian 1 PBX 11.

```

REQ: prt
TYPE: 2616
TN 5 16
DES
DES Remote site 1
TN 005 0 00 16
TYPE 2616
CDEN 8D
CUST 0
AOM 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
CLS CTD FBD WTD LPR MTD FND HTD ADD HFD
    MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD DTA DRG1
    POD DSX VMD CMSD CCSD SWD LND CNDD
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
    ICDD CDMD LLCN MCTD CLBD AUTU
    GPUD DPUD DNDD CFXD ARHD CLTD ASCD
    CPFA CPTA ABDD CFHD FICD NAID BUZZ AHD
    DDGA NAMA
    DRDD EXR0
    USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3

```

← Telephone type

← RLC slot and port numbers

TGAR must be configured to allow trunk access. Refer to your PBX documentation for more details.

DTA defines the port as a data port.


```
TOV 0 MINS
DTAO MCA
PSEL DMDM
HUNT
PSDS NO
TRAN ASYN
PAR SPACE
DTR ON
DUP FULL
HOT OFF
AUT ON
BAUD 9600
DCD ON
PRM KBD ON
VLL OFF
MOD YES
INT OFF
CLK OFF
KBD ON
RTS OFF
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY 00 SCR 1234 0 MARP
    01
    02
    03
    04
    05
    06
    07
    08
    09
    10
    11
    12
    13
    14
    15
```

← Network ports must be defined as MCA.

↑ The number that the Remote Gateway 9150 unit needs to connect to the RLC. It must be a DID number.

RLC configuration

This section shows the configuration settings for the RLC. You can obtain a similar configuration printout by performing a configuration download while connected to the RLC.

Note: Configuration settings are separated by commas (.).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 391.

```

IPCFCFG 10.2.1.1,255.255.0.0,10.2.1.10,10.3.1.2,255.255.0.0

APPMODCFG 0,NC,NC
APPMODCFG 1,E,G729A,G729A
APPMODCFG 2,NC,NC
APPMODCFG 3,NC,NC
APPMODCFG 4,NC,NC
APPMODCFG 5,NC,NC
APPMODCFG 6,NC,NC
APPMODCFG 7,NC,NC

SYSCFG 1,HOST1

RLCCFG E,E
ACCFG D

PORTCFG 0,1,0,2,2,D
PORTCFG 1,1,0,2,2,D
PORTCFG 2,1,0,2,2,D
PORTCFG 3,1,0,2,2,D
PORTCFG 4,1,0,2,2,D
PORTCFG 5,1,0,2,2,D

```

RLC's IP address information:

- IP address
- Subnet mask
- IP gateway
- Management IP address
- Management subnet mask

DSP application module
(only module 1 is configured in this case)

Unit ID and node name

Ports configured as remote ports

```

PORTCFG 6,0
PORTCFG 7,0
PORTCFG 8,0
PORTCFG 9,0
PORTCFG 10,0
PORTCFG 11,0
PORTCFG 12,0
PORTCFG 13,0
PORTCFG 14,0
PORTCFG 15,0

PORTCFG 16,2,2,6065556987
PORTCFG 17,0
PORTCFG 18,0
PORTCFG 19,0
PORTCFG 20,0
PORTCFG 21,0
PORTCFG 22,0
PORTCFG 23,0
PORTCFG 24,0
PORTCFG 25,0
PORTCFG 26,0
PORTCFG 27,0
.
.
.
PORTCFG 63,0

RUNITCFG 1,E,0,2,45,45,3,1234567890,0987654321,E,Y,10.1.1.2,
          E,16,D,16,10,Y,6065556987,D
RUNITCFG 2,D,0,0,2,1,1,D,D,D
RUNITCFG 3,D,0,0,2,1,1,D,D,D
RUNITCFG 4,D,0,0,2,1,1,D,D,D
RUNITCFG 5,D,0,0,2,1,1,D,D,D
RUNITCFG 6,D,0,0,2,1,1,D,D,D
RUNITCFG 7,D,0,0,2,1,1,D,D,D
RUNITCFG 8,D,0,0,2,1,1,D,D,D
RUNITCFG 9,D,0,0,2,1,1,D,D,D
RUNITCFG 10,D,0,0,2,1,1,D,D,D

```

Ports configured as local ports

Port configured as network port

Remote unit connection information (unit 1):

- remote unit number
- 9150's unit ID
- security information (inbound and outbound security IDs)
- remote unit's IP address
- network port
- PSTN number

```
ONOFFCFG 1,SUN,0 00:00
ONOFFCFG 1,MON,0 00:00
ONOFFCFG 1,TUE,0 00:00
ONOFFCFG 1,WED,0 00:00
ONOFFCFG 1,THU,0 00:00
ONOFFCFG 1,FRI,0 00:00
ONOFFCFG 1,SAT,0 00:00
ONOFFCFG 2,SUN,0 00:00
ONOFFCFG 2,MON,0 00:00
ONOFFCFG 2,TUE,0 00:00
ONOFFCFG 2,WED,0 00:00
ONOFFCFG 2,THU,0 00:00
ONOFFCFG 2,FRI,0 00:00
ONOFFCFG 2,SAT,0 00:00
ONOFFCFG 3,SUN,0 00:00
ONOFFCFG 3,MON,0 00:00
ONOFFCFG 3,TUE,0 00:00
ONOFFCFG 3,WED,0 00:00
ONOFFCFG 3,THU,0 00:00
ONOFFCFG 3,FRI,0 00:00
ONOFFCFG 3,SAT,0 00:00
ONOFFCFG 4,SUN,0 00:00
ONOFFCFG 4,MON,0 00:00
ONOFFCFG 4,TUE,0 00:00
ONOFFCFG 4,WED,0 00:00
ONOFFCFG 4,THU,0 00:00
ONOFFCFG 4,FRI,0 00:00
ONOFFCFG 4,SAT,0 00:00
ONOFFCFG 5,SUN,0 00:00
ONOFFCFG 5,MON,0 00:00
ONOFFCFG 5,TUE,0 00:00
ONOFFCFG 5,WED,0 00:00
ONOFFCFG 5,THU,0 00:00
ONOFFCFG 5,FRI,0 00:00
ONOFFCFG 5,SAT,0 00:00
ONOFFCFG 6,SUN,0 00:00
ONOFFCFG 6,MON,0 00:00
ONOFFCFG 6,TUE,0 00:00
ONOFFCFG 6,WED,0 00:00
ONOFFCFG 6,THU,0 00:00
ONOFFCFG 6,FRI,0 00:00
```

← Online/offline schedule

```
ONOFFCFG 6,SAT,0 00:00
ONOFFCFG 7,SUN,0 00:00
ONOFFCFG 7,MON,0 00:00
ONOFFCFG 7,TUE,0 00:00
ONOFFCFG 7,WED,0 00:00
ONOFFCFG 7,THU,0 00:00
ONOFFCFG 7,FRI,0 00:00
ONOFFCFG 7,SAT,0 00:00
ONOFFCFG 8,SUN,0 00:00
ONOFFCFG 8,MON,0 00:00
ONOFFCFG 8,TUE,0 00:00
ONOFFCFG 8,WED,0 00:00
ONOFFCFG 8,THU,0 00:00
ONOFFCFG 8,FRI,0 00:00
ONOFFCFG 8,SAT,0 00:00
ONOFFCFG 9,SUN,0 00:00
ONOFFCFG 9,MON,0 00:00
ONOFFCFG 9,TUE,0 00:00
ONOFFCFG 9,WED,0 00:00
ONOFFCFG 9,THU,0 00:00
ONOFFCFG 9,FRI,0 00:00
ONOFFCFG 9,SAT,0 00:00
ONOFFCFG 10,SUN,0 00:00
ONOFFCFG 10,MON,0 00:00
ONOFFCFG 10,TUE,0 00:00
ONOFFCFG 10,WED,0 00:00
ONOFFCFG 10,THU,0 00:00
ONOFFCFG 10,FRI,0 00:00
ONOFFCFG 10,SAT,0 00:00
```

```
FBQOSCFG 1,E,5,6,5,10,10,32
FBQOSCFG 2,D,5,6,5,10,10,32
FBQOSCFG 3,D,5,6,5,10,10,32
FBQOSCFG 4,D,5,6,5,10,10,32
FBQOSCFG 5,D,5,6,5,10,10,32
FBQOSCFG 6,D,5,6,5,10,10,32
FBQOSCFG 7,D,5,6,5,10,10,32
FBQOSCFG 8,D,5,6,5,10,10,32
FBQOSCFG 9,D,5,6,5,10,10,32
FBQOSCFG 10,D,5,6,5,10,10,32
```

Item not Configured

Quality of Service settings
(these are default settings)

Caller ID (not configured; one
line for each remote unit)

Remote Gateway 9150 unit configuration

This section shows the configuration settings for the Remote Gateway 9150 unit. You can obtain a similar configuration printout by performing a configuration download while connected to the Remote Gateway 9150 unit.

Note: Configuration settings are separated by commas (.).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 391.

```

IPCFCFG 10.1.1.2,255.255.0.0,10.1.1.10
APPMODCFG 0,SPARE,TSIDSP
APPMODCFG 1,E,G729A,G729A
APPMODCFG 2,NC,NC
APPMODCFG 3,NC,NC
APPMODCFG 4,1,1,E,1,1,5556987,60655569870101,E,1,1,
5556988,60655569880101
APPMODCFG 5,NC,NC
APPMODCFG 6,NC,NC
APPMODCFG 7,NC,NC
SYSCFG 2, Remote site 1
ROUCFG 13:00,0,JAN-13-2000,911,#222,#333,#345,#456,E
ACCFG N

```

9150 unit's IP interface information:

- IP address
- Subnet mask
- IP gateway

On-board DSP module (module 0) and installed DSP application module (module 1)

ISDN BRI module configuration

- module number
- PSTN number for each B-channel
- SPID for each B-channel

Unit ID and node name

System configuration:

- Emergency service number
- System date and time
- SPRE codes

```
RLCDETCFG 1,3,0987654321,1234567890,E,10.2.1.1,E,6135551234,E,D
```

Host PBX connection
information:

- RLC's unit ID
- security information
(inbound and outbound
security IDs)
- RLC's IP address
- RLC PSTN number

```
ROUDEVCFG 0,2,0,E,E,E,Bryan Dion,8734,04
ROUDEVCFG 1,2,1,E,E,E,Marc Horman,8707,04
ROUDEVCFG 2,2,2,E,E,E,Brad McAllister,8708,04
ROUDEVCFG 3,2,3,E,E,E,Andrew Wong,8760,04
ROUDEVCFG 4,2,4,E,E,E,Corey Smith,8709,04
ROUDEVCFG 5,2,5,E,E,E,Tracey Black,8743,04
ROUDEVCFG 6,0,E,E,E,John Brown,8611,04
ROUDEVCFG 7,1,0
ROUDEVCFG 8,1,0
ROUDEVCFG 9,1,0
ROUDEVCFG 10,1,0
ROUDEVCFG 11,1,0
ROUDEVCFG 12,1,0
ROUDEVCFG 13,1,0
ROUDEVCFG 14,1,0
ROUDEVCFG 15,1,0
ROUDEVCFG 16,1,0
ROUDEVCFG 17,1,0
ROUDEVCFG 18,1,0
ROUDEVCFG 19,1,0
ROUDEVCFG 20,1,0
ROUDEVCFG 21,1,0
ROUDEVCFG 22,1,0
ROUDEVCFG 23,1,0
ROUDEVCFG 24,1,0
ROUDEVCFG 25,1,0
ROUDEVCFG 26,1,0
ROUDEVCFG 27,1,0
ROUDEVCFG 28,1,0
ROUDEVCFG 29,1,0
ROUDEVCFG 30,1,0
ROUDEVCFG 31,1,0
ROUDEVCFG 32,2,31,E,E,E,FAX,8664,900
```

Port (station) configuration:

- Port number
- Local and remote capability
- CPND
- DN
- Restricted digits

Unconfigured ports

Note: The default capability is Remote.

Fax port configuration:

- Port number
- Local and remote capability
- CPND
- DN
- Restricted digits

```

FKEYCFG 0,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 1,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 2,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 3,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 4,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 5,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 6,8 LC1 ,9 LC2 ,NC
FKEYCFG 7,NC
FKEYCFG 8,NC
FKEYCFG 9,NC
FKEYCFG 10,NC
FKEYCFG 11,NC
FKEYCFG 12,NC
FKEYCFG 13,NC
FKEYCFG 14,NC
FKEYCFG 15,NC
FKEYCFG 16,NC
FKEYCFG 17,NC
FKEYCFG 18,NC
FKEYCFG 19,NC
FKEYCFG 20,NC
FKEYCFG 21,NC
FKEYCFG 22,NC
FKEYCFG 23,NC
FKEYCFG 24,NC
FKEYCFG 25,NC
FKEYCFG 26,NC
FKEYCFG 27,NC
FKEYCFG 28,NC
FKEYCFG 29,NC
FKEYCFG 30,NC
FKEYCFG 31,NC
FKEYCFG 32,NC

```

Local station feature keys configuration:

- Port number
- Feature key number
- Feature name
- DN (if applicable)
- locations of local call appearance keys 1 and 2

Trunk group configuration:

- Trunk group number
- Trunk access code
- B-channels (ISDN module and B-channel number)
- DNs to alert

```

TRKGRPCFG 1,E,#61,4.0.0 4.0.1,8739
TRKGRPCFG 2,D,#62,1.0.0 1.0.1 2.0.0 2.0.1,4002
TRKGRPCFG 3,D,#63,1.0.0 1.0.1 2.0.0 2.0.1,4004
TRKGRPCFG 4,D,#64,1.0.0 1.0.1 2.0.0 2.0.1,4006
TRKGRPCFG 5,D,#65,1.0.0 1.0.1 2.0.0 2.0.1,4008
TRKGRPCFG 6,D,#66,1.0.0 1.0.1 2.0.0 2.0.1,4010
TRKGRPCFG 7,D,#67,1.0.0 1.0.1 2.0.0 2.0.1,4012
TRKGRPCFG 8,D,#68,1.0.0 1.0.1 2.0.0 2.0.1,4014

```

Item not Configured

Caller ID (not configured)

Appendix C

Pin-out tables for connections

In this appendix

TELCO 1 connector pin-out table	404
TELCO 2 connector pin-out table	406
Ethernet connector pin-out table	408
Admin (serial) connector pin-out table	409
Power connector pin-out table	410

TELCO 1 connector pin-out table

Note: The colors shown in this table represent standard telephone cable pin-outs.

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Digital port 0	1	DP 0 RING	BL-W	26	DP 0 TIP	W-BL
Digital port 1	2	DP 1 RING	OR-W	27	DP 1 TIP	W-OR
Digital port 2	3	DP 2 RING	GR-W	28	DP 2 TIP	W-GR
Digital port 3	4	DP 3 RING	BR-W	29	DP 3 TIP	W-BR
Digital port 4	5	DP 4 RING	SL-W	30	DP 4 TIP	W-SL
Digital port 5	6	DP 5 RING	BL-R	31	DP 5 TIP	R-BL
Digital port 6	7	DP 6 RING	OR-R	32	DP 6 TIP	R-OR
Digital port 7	8	DP 7 RING	GR-R	33	DP 7 TIP	R-GR
Digital port 8	9	DP 8 RING	BR-R	34	DP 8 TIP	R-BR
Digital port 9	10	DP 9 RING	SL-R	35	DP 9 TIP	R-SL
Digital port 10	11	DP 10 RING	BL-B	36	DP 10 TIP	B-BL
Digital port 11	12	DP 11 RING	OR-B	37	DP 11 TIP	B-OR
Digital port 12	13	DP 12 RING	GR-B	38	DP 12 TIP	B-GR
Digital port 13	14	DP 13 RING	BR-B	39	DP 13 TIP	B-BR
Digital port 14	15	DP 14 RING	SL-B	40	DP 14 TIP	B-SL
Digital port 15	16	DP 15 RING	BL-Y	41	DP 15 TIP	Y-BL
Leave open for UL spacing requirements	17	Open	OR-Y	42	Open	Y-OR
Module 4 (ISDN BRI—ST only)	18	MOD 3 Tip 0+	GR-Y	43	Module 3 Tip 0-	Y-GR

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Module 4 (ISDN BRI—U or ST)	19	MOD 3 Ring 0+	BR-Y	44	Module 3 RING 0-	Y-BR
Module 5 (ISDN BRI—ST only)	20	MOD 4 Tip 0+	SL-Y	45	Module 4 Tip 0-	Y-SL
Module 5 (ISDN BRI—U or ST)	21	MOD 4 Ring 0+	BL-V	46	Module 4 RING 0-	V-BL
Module 5 (for future use)	22	MOD 4 Tip 1+	OR-V	47	Module 4 TIP 1-	V-OR
Module 5 (for future use)	23	MOD 4 Ring 1+	GR-V	48	Module 4 RING 1-	V-GR
Leave open for UL spacing requirements	24	Open	BR-V	49	UK Ring	V-BR
Analog port	25	AP TIP	SL-V	50	AP RING	V-SL

TELCO 2 connector pin-out table

Note: The colors shown in this table represent standard telephone cable pin-outs.

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Digital port 16	1	DP 16 RING	BL-W	26	DP 16 TIP	W-BL
Digital port 17	2	DP 17 RING	OR-W	27	DP 17 TIP	W-OR
Digital port 18	3	DP 18 RING	GR-W	28	DP 18 TIP	W-GR
Digital port 19	4	DP 19 RING	BR-W	29	DP 19 TIP	W-BR
Digital port 20	5	DP 20 RING	SL-W	30	DP 20 TIP	W-SL
Digital port 21	6	DP 21 RING	BL-R	31	DP 21 TIP	R-BL
Digital port 22	7	DP 22 RING	OR-R	32	DP 22 TIP	R-OR
Digital port 23	8	DP 23 RING	GR-R	33	DP 23 TIP	R-GR
Digital port 24	9	DP 24 RING	BR-R	34	DP 24 TIP	R-BR
Digital port 25	10	DP 25 RING	SL-R	35	DP 25 TIP	R-SL
Digital port 26	11	DP 26 RING	BL-B	36	DP 26 TIP	B-BL
Digital port 27	12	DP 27 RING	OR-B	37	DP 27 TIP	B-OR
Digital port 28	13	DP 28 RING	GR-B	38	DP 28 TIP	B-GR
Digital port 29	14	DP 29 RING	BR-B	39	DP 29 TIP	B-BR
Digital port 30	15	DP 30 RING	SL-B	40	DP 30 TIP	B-SL
Digital port 31	16	DP 31 RING	BL-Y	41	DP 31 TIP	Y-BL
Leave open for UL spacing requirements	17	Open	OR-Y	42	Open	Y-OR
Module 6 (ISDN BRI—ST only)	18	MOD 5 Tip 0+	GR-Y	43	Module 5 Tip 0-	Y-GR

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Module 6 (ISDN BRI—U or ST)	19	MOD 5 Ring 0+	BR-Y	44	Module 5 Ring 0-	Y-BR
Module 7 (ISDN BRI—ST only)	20	MOD 6 Tip 0+	SL-Y	45	Module 6 Tip 0-	Y-SL
Module 7 (ISDN BRI—U or ST)	21	MOD 6 Ring 0+	BL-V	46	Module 6 Ring 0-	V-BL
Module 7 (for future use)	22	MOD 6 Tip 1+	OR-V	47	Module 6 Tip 1-	V-OR
Module 7 (for future use)	23	MOD 6 Ring 1+	GR-V	48	Module 6 Ring 1-	V-GR
Leave open for UL spacing requirements	24	Open	BR-V	49	Open	V-BR
Fault Relay Contact 1	25	UNUSED		50	UNUSED	

Ethernet connector pin-out table

Pin number	Signal name	I/O	Description
1	TX+	O	Transmit Clock +
2	TXC	I	Transmit Clock Common (Ground)
3	TX-	O	Transmit Clock -
4	Chassis Ground	I	Shield
5	Chassis Ground	I	Shield
6	RXC	I	Receive Clock Common (Ground)
7	RX+	I	Receive Clock +
8	RX-	I	Receive Clock -

Admin (serial) connector pin-out table

Pin number	Signal name	I/O	Description
1			
2	MMI-RXD	I	MMI RS-232C Receive Data
3	MMI-TXD	O	MMI RS-232C Transmit Data
4			
5	Ground	I	Logic Ground
6			
7			
8			
9			

Power connector pin-out table

Pin number	Signal name	I/O	Current	Description
1	+5V	I	5.0 A	+5v
2	Ground	I		Logic Ground
3	+24V	I	1.5 A	+24v
4	-12V	I	0.1 A	+24v

Appendix D

Display log definitions

In this appendix

Display logs	412
--------------	-----

Display logs

The display log functionality is significantly improved over prior releases of Remote Gateway 9150. This appendix lists the 9150 system's display log error and status messages.

Statistic	Definition
LOG NUMBER	0
DESCRIPTION	This is a description of the log that is being generated.
SEVERITY	NORMAL, WARNING, MINOR, MAJOR, CRITICAL (Assigns one of these levels to the Log.)
TASK	This is the task that originates the trap. This can be the full name or an abbreviation. (For development use only.)
PRODUCT	RLC, 9150, 911x (Lists all products that can generate this log.)
CANCELLATION	This is a cross-reference to another log number that is the complement of the current log (for example, QOS Transition/ Recovery, Link Up/Down.) This consists of a LOG NUMBER and send Log IDType.
ACTION TO BE TAKEN:	If the Severity is higher than NORMAL, this normally contains information that would help the end user correct the problem, if possible (for example, a Configuration Change), or give them information about where the user can go for help.
PARAMETERS	1) description of parameter 1 2) description of parameter 2 . . . N) description of parameter N
DISPLAYED TEXT	This information describing the event that led to the occurrence of this log appears in the Display Logs pop-up window.
PRODUCES HOST PBX ALARM AND ALERT	This information indicates whether the host PBX produces an alarm and alert.

Statistic	Definition
LOG NUMBER	1
DESCRIPTION	This log indicates that the system started.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Version string
DISPLAYED TEXT	System started. S/W Version - P1
LOG NUMBER	2
DESCRIPTION	This logs indicates that there was a failure in allocation of the TCM block.
SEVERITY	CRITICAL
TASK	None
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	TCM buffer is exhausted. If the problem persists re-boot the system and report back to vendor.
PARAMETERS	None
DISPLAYED TEXT	Out of TCM buffer

Statistic	Definition
LOG NUMBER	3
DESCRIPTION	This logs indicates that there was a failure in allocation of memory of size 'n'.
SEVERITY	MAJOR
TASK	None
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Memory buffers exhausted. If the problem persists re-boot the system.
PARAMETERS	1) Size of memory block that the system failed to allocate
DISPLAYED TEXT	Couldn't allocate memory of size P1

LOG NUMBER	4
DESCRIPTION	This logs indicates that there was a failure in sending a message to a Remote Gateway 9100 Series unit.
SEVERITY	MAJOR
TASK	None
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) The destination host is unreachable check its status. 2) Check the configuration.
PARAMETERS	1) Unit ID of remote board for which message was intended
DISPLAYED TEXT	Couldn't send message to unit ID: P1

Statistic	Definition
LOG NUMBER	5
DESCRIPTION	This log indicates that the QoS of the IP network degraded and the system transitioned to the PSTN.
SEVERITY	NORMAL
TASK	QoS Transitioning
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 2 - FB_RECOVERY_LOG_ID
ACTION TO BE TAKEN	Investigate why the IP network was determined to be below VoIP quality. Review the Engineering Guidelines.
PARAMETERS	1) Unit ID of the Remote Gateway 9100 Series unit for which the IP QoS has degraded
DISPLAYED TEXT	Transition to Remote Site: P1
PRODUCES HOST PBX ALARM AND ALERT	Yes
LOG NUMBER	6
DESCRIPTION	This log indicates that the QoS of the IP network recovered and the system transitioned to the IP Network.
SEVERITY	NORMAL
TASK	Fallback
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 1 - FB_FALLBACK_LOG_ID
ACTION TO BE TAKEN	Investigate why the IP network was determined to be below VoIP quality. Review the Engineering Guidelines.
PARAMETERS	1) Unit ID of the Remote Gateway 9100 Series unit for which the IP QOS has recovered
DISPLAYED TEXT	Recovery to Remote Site: P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	7
DESCRIPTION	This log indicates that a user logged onto the system.
SEVERITY	NORMAL
TASK	Session Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 8
ACTION TO BE TAKEN	None
PARAMETERS	1) Connection (serial or Telnet) through which user logged onto system
DISPLAYED TEXT	User logged on: P1

LOG NUMBER	8
DESCRIPTION	This log indicates that a user logged off from the system.
SEVERITY	NORMAL
TASK	Session Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 7
ACTION TO BE TAKEN	None
PARAMETERS	1) Logoff type – normal or terminated
DISPLAYED TEXT	User logged off: P1

Statistic	Definition
LOG NUMBER	9
DESCRIPTION	This log indicates that logon to the system failed.
SEVERITY	WARNING
TASK	Session Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Reason – wrong user name, password, device busy, and so on
DISPLAYED TEXT	User login failed: P1
LOG NUMBER	10
DESCRIPTION	This log indicates a debug Session Terminated. A debug session that was inactive for more than 15 minutes was automatically logged off from the system.
SEVERITY	NORMAL
TASK	Session Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Reason for termination
DISPLAYED TEXT	Debug session terminated: P1

Statistic	Definition
LOG NUMBER	11
DESCRIPTION	This log indicates that database reading from Flash at Power on failed. This can be caused by corrupted Flash. As a result, the system starts with the default configuration.
SEVERITY	CRITICAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Re-configure the system and then save it to Flash. Note: When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds. 2) Restart the system and log into the system and check the configured parameters. If the problem persists contact your vendor.
PARAMETERS	1) Reason reading from Flash failed
DISPLAYED TEXT	Database reading from Flash failed - P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	12
DESCRIPTION	This log indicates that user tried saving a new configuration to Flash.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status of Save to Flash – success or failure
DISPLAYED TEXT	Database save to Flash: P1

LOG NUMBER	13
DESCRIPTION	This log indicates that a user defaulted the configuration of the board using the Set default configuration command.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Database defaulted

Statistic	Definition
LOG NUMBER	14
DESCRIPTION	This log indicates that User tried a configuration upload.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status - success or failure 2) Name of configuration file 3) IP address of source of configuration file
DISPLAYED TEXT	Database upload: P1 (P2 from P3)
LOG NUMBER	15
DESCRIPTION	This log indicates that an application module is enabled and not plugged in. This can happen when the user configures a module and then removes it from the system.
SEVERITY	MAJOR
TASK	MMI
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	Re-configure the application module and plug it in again.
PARAMETERS	1) Module type 2) Mismatch details
DISPLAYED TEXT	Application module configuration mismatch: P1 P2

Statistic	Definition
LOG NUMBER	16
DESCRIPTION	<p>This log indicates that there is a DN clash. This can happen for the following reasons:</p> <ul style="list-style-type: none">■ One DN is configured for multiple ports■ One access code is configured for trunk groups■ One SPRE code is configured for different functions■ A longer DN number exists
SEVERITY	MAJOR
TASK	MMI
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	Check for duplication of configuration (Use "Get DN List" to see the data) and correct it.
PARAMETERS	<ol style="list-style-type: none">1) Type of Data2) First clashing port number3) Second clashing port number
DISPLAYED TEXT	DN clash: P1 P2 P3

Statistic	Definition
LOG NUMBER	17
DESCRIPTION	This log indicates that the user tried to upload software. This could be application software or ISDN module software. After an application software upload, the system is normally restarted. Therefore, it is possible that this log was lost.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status - success or failure 2) Module type - application or ISDN 3) File name 4) Source of file (for example, IP address)
DISPLAYED TEXT	Software upload: P1 (P2, P3 from P4)
LOG NUMBER	18
DESCRIPTION	This log indicates that a user tried a cross connection to the host PBX over RS232 Port using the XConnect command.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status of cross-connect attempt - success or failure
DISPLAYED TEXT	User cross connect to PBX: P1

Statistic	Definition
LOG NUMBER	19
DESCRIPTION	This log indicates that a user tried a Remote connection to another system using the Telnet command.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status of Telnet attempt - success or failure 2) Destination (for example, IP address)
DISPLAYED TEXT	User remote connection: P1 P2
LOG NUMBER	20
DESCRIPTION	This log indicates the power on initialization of the ports completed.
SEVERITY	NORMAL
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Power-on initialization of ports completed

Statistic	Definition
LOG NUMBER	21
DESCRIPTION	This log indicates that the remote site re-initialized upon Remote Gateway 9100 Series unit configuration change.
SEVERITY	NORMAL
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Unit ID of the Remote Gateway 9100 Series unit re-initialized
DISPLAYED TEXT	Remote site: P1 is re-initialized
LOG NUMBER	22
DESCRIPTION	This log signals that the link to the specified Remote Gateway 9100 Series unit went down.
SEVERITY	MAJOR
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for transport medium (IP or PSTN) connectivity and configuration. 2) If medium is PSTN, check BRI status on the PBX. 3) If transport medium connectivity is OK, but the problem continues, then re-boot the RLC and the remote unit. 4) If the problem persists, contact your vendor.
PARAMETERS	1) Unit ID of the Remote Gateway 9100 Series unit to which the link went down
DISPLAYED TEXT	Link down for Remote Site: P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	23
DESCRIPTION	This log indicates that a Remote Gateway 9100 Series unit registered.
SEVERITY	NORMAL
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Unit ID of the Remote Gateway 9100 Series unit that registered
DISPLAYED TEXT	Remote site: P1 is registered
LOG NUMBER	24
DESCRIPTION	This log signals a port registration clash for a dedicated port.
SEVERITY	WARNING
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	Possible mis-configuration on remote. Check the configurations.
PARAMETERS	1) Port number of first clashing remote port 2) Unit ID of the remote on which first clashing port resides 3) Number of dedicated RLC port for which there is a clash 4) Port number of second clashing remote port 5) Unit ID of the remote on which the second clashing port resides
DISPLAYED TEXT	Registration clash for port P1 on Remote Site: P2 with port P3 on the RLC. Dedicated port P3 is already registered with port P4 of the Remote Site: P5

Statistic	Definition
LOG NUMBER	25
DESCRIPTION	This log indicates that a remote port registered with a multi-user/dynamic RLC port.
SEVERITY	NORMAL
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Port number of remote port registered on multi-user/dynamic port 2) Unit ID of remote on which remote port resides 3) Port number of multi-user/dynamic port on RLC
DISPLAYED TEXT	Port P1 on Remote Site: P2 is registered with multi-user /dynamic pool port P3

Statistic	Definition
LOG NUMBER	26
DESCRIPTION	This log indicates a port registration clash for a multi-user port.
SEVERITY	WARNING
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	<ol style="list-style-type: none"> 1) Make sure that this port is not registered with any other remote unit. 2) If the port is already registered with another remote unit, determine to which remote unit the port needs to be registered. 3) If you need to register the port with a remote unit other than the one it is currently registered to, change the configuration and re-boot the RLC and the remote unit.
PARAMETERS	<ol style="list-style-type: none"> 1) Number of remote port for which there is a registration clash 2) Unit ID of the Remote Gateway 9100 Series unit on which port resides 3) Port number of multi-user port on RLC 4) Port number of currently registered remote port 5) Unit ID of the Remote Gateway 9100 Series unit on which currently registered port resides
DISPLAYED TEXT	Registration clash for port P1 on Remote Site: P2 with multi-user port P3. Multi-user port P3 is already registered with port P4 on Remote Site P5

Statistic	Definition
LOG NUMBER	27
DESCRIPTION	This log indicates that a port registration failed for a dynamic pool port. All ports in this dynamic pool are registered and no port is available for use.
SEVERITY	WARNING
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	<ol style="list-style-type: none">1) Make sure that this port is not registered with any other remote unit.2) If the port is already registered with another remote unit, determine to which remote unit the port needs to be registered.3) If you need to register the port with a remote unit other than the one it is currently registered to, change the configuration and re-boot the RLC and the remote unit.
PARAMETERS	<ol style="list-style-type: none">1) Port number on remote for which there is a registration failure2) Unit ID of the Remote Gateway 9100 Series unit on which port resides
DISPLAYED TEXT	Registration failed for dynamic pool port P1 on Remote Site: P2

Statistic	Definition
LOG NUMBER	28
DESCRIPTION	This logs indicates that there was a failure in allocation of a new call register.
SEVERITY	CRITICAL
TASK	Device Control, Call Processing
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	The system memory allocation has failed and might have been exhausted. If the problem persists re-boot the system.
PARAMETERS	1) Port number
DISPLAYED TEXT	Call register allocation failed in local calling on Port P1

Statistic	Definition
LOG NUMBER	29
DESCRIPTION	This log indicates that there were insufficient DSP channels when a voice call was attempted.
SEVERITY	MINOR
TASK	Device Control/Call Processing
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) All the DSP channels on the system are in use. Wait for calls to be dropped. 2) To avoid blocking, either distribute calls onto additional RLCs and 9150s, or add DSP modules to existing equipment, provided there is space available for additional modules. Otherwise action # 1 applies.
PARAMETERS	1) Port number
DISPLAYED TEXT	DSP resource allocation failed on Port P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	30
DESCRIPTION	This log indicates that allocation of a local trunk for a local call failed. The possible reasons for failure are: 1) All the trunks are in use. 2) There are no Local or Local/Remote trunks configured. 3) The BRI link may be down or the BRI module might not be plugged in completely.
SEVERITY	MINOR
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Confirm that the BRI modules are plugged in properly and the BRI link is UP. 2) Confirm that the BRI configuration is correct.
PARAMETERS	1) Port number
DISPLAYED TEXT	Local trunk allocation failed on port P1

Statistic	Definition
LOG NUMBER	31
DESCRIPTION	This log indicates that a local call failed because the dialed DN didn't exist.
SEVERITY	WARNING
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Verify the dialed digits with the configuration numbers.
PARAMETERS	1) Dialed digits
DISPLAYED TEXT	Unassigned number P1

LOG NUMBER	32
DESCRIPTION	This log indicates that a local call failed because the sequence of dialed digits is not allowed on the set that is attempting to place the call.
SEVERITY	WARNING
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Verify that the dialed digits don't match the disabled outbound digits.
PARAMETERS	1) Dialed digits
DISPLAYED TEXT	Disabled outbound digits blocked P1

Statistic	Definition
LOG NUMBER	33
DESCRIPTION	This log indicates that the DSP cross connect failed, which might have resulted in no voice path being established.
SEVERITY	CRITICAL
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Contact the vendor if the problem persists.
PARAMETERS	1) Port number
DISPLAYED TEXT	DSP cross connect failed on port P1
LOG NUMBER	34
DESCRIPTION	This log indicates a change in the system mode.
SEVERITY	NORMAL
TASK	Device Control, Call Processing
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status: online/offline
DISPLAYED TEXT	Changing system mode to: P1

Statistic	Definition
LOG NUMBER	35
DESCRIPTION	This log indicates that there was a failure in registering to a remote RLC. This would indicate that the Host is unreachable through both the IP and the PSTN.
SEVERITY	MAJOR
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for the IP/PSTN connectivity. 2) Check for the remote Host status. 3) Check the correctness of configuration. Units must be enabled.
PARAMETERS	1) Unit ID of remote site to which registration failed
DISPLAYED TEXT	Failed to register to Remote Site: P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	36
DESCRIPTION	This log indicates the success or failure of a Remote Gateway 9150 unit port's attempt to register with a multi-user/dynamic port on a RLC.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	1) Determine if the port was in use. 2) Configure the port as a multi-user/dynamic port. 3) The host RLC is unreachable.
PARAMETERS	1) 9150 unit's port number attempting to register with the multi-user/dynamic port on the RLC 2) Registered or unregistered status of 9150 unit's port 3) Port number of multi-user/dynamic port on RLC
DISPLAYED TEXT	ROU port P1, P2 to RLC port P3

Statistic	Definition
LOG NUMBER	37
DESCRIPTION	<p>This log indicates that an attempt to connect to a Remote Gateway 9100 Series unit on the specified medium failed.</p> <ol style="list-style-type: none"> 1) If the same message is displayed with both IP and PSTN, in succession, the specified remote cannot be reached. 2) If only one message displays with a specific medium while connections on other medium are fine, it indicates a possible attempt to connect on the medium due to: <ol style="list-style-type: none"> a) Priority of the call that requires only that medium. Voice call would have failed. Check for log number 55. b) IP QoS state and priority level required a first attempt on the specified medium. A voice call would have succeeded on the other medium, though it cannot be guaranteed. c) Attempt was made on receiving a QoS status message.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	<p>Verify the following:</p> <ol style="list-style-type: none"> 1) Correctness of configurations 2) Whether the network connections are proper 3) Status of the remote board
PARAMETERS	<ol style="list-style-type: none"> 1) Remote Gateway 9100 Series unit ID 2) Medium on which the attempt failed
DISPLAYED TEXT	Not able to connect to Remote Site: P1 on P2 medium
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	38
DESCRIPTION	<p>This log indicates that an attempt to bring up an additional trunk failed due to the lack of an unoccupied, configured trunk.</p> <p>This could cause the failure of a voice call depending on the media allowed to communicate to that remote, the priority of the call, and the Extra Bandwidth configured.</p> <p>However, verify the presence of log number 55 on the RLC to see if a voice call did not succeed. Look for the presence of log number 37 on the RLC. It indicates that an attempt was made to connect the voice call on that medium, but that the medium was not reachable.</p>
SEVERITY	MINOR
TASK	Network Manager
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	Verify for the specified log numbers and note them. If this happens frequently, new trunks may have to be added.
PARAMETERS	1) Remote Gateway 9100 Series unit ID
DISPLAYED TEXT	No free additional trunk available to Remote Site: P1

Statistic	Definition
LOG NUMBER	39
DESCRIPTION	<p>This log indicates that there an attempt was made to get an additional trunk on the PSTN.</p> <p>This message has a corresponding message with same number on the Remote Gateway 9150 unit board. This can cause a voice call to fail, depending on the media allowed to communicate with that remote device and the priority of the call.</p> <p>However, check for the presence of log number 55 on the RLC to see if a voice call did not succeed. Look for the presence of log number 37 on the RLC. It indicates that an attempt was made to connect the voice call on that medium, but that the medium was not reachable.</p>
SEVERITY	MINOR
TASK	Network Manager
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	<ol style="list-style-type: none">1) Ensure the PSTN numbers shown in Trunk Configuration are correct on both the RLC and Remote Gateway 9150 unit.2) Ensure the trunk route to that Remote Gateway 9100 Series unit is not busy.
PARAMETERS	<ol style="list-style-type: none">1) Remote Gateway 9100 Series unit ID2) PSTN number attempted3) A flag to indicate whether attempt is made by remote board or local board.<ol style="list-style-type: none">a) indicates attempt made by local boardb) indicates attempt made by remote board
DISPLAYED TEXT	Attempt to bring-up additional trunk failed. Remote P1, PSTN number P2, flag P3
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	40
DESCRIPTION	This log indicates that an attempt to transition to the PSTN failed. Appearance of this message does not cause a voice call to drop. However, if RLC log numbers 42 or 56 display, the system can drop voice calls and not be able to connect to the Remote Gateway 9100 Series unit temporarily.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	1) Look for correctness of primary PSTN number. If PSTN is disabled, ignore this message 2) Trunk route might be busy to that remote. 3) If the specified logs also display, IP network could be down
PARAMETERS	1) Remote Gateway 9100 Series unit ID
DISPLAYED TEXT	Transition did not happen to Remote Site: P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	41
DESCRIPTION	This log indicates the failure of the system to connect to the specified remote on the IP network due to a network problem other than unacceptable QoS.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for problems on the IP network. 2) Wait for more attempts because connections can take more time depending on nature of the network.
PARAMETERS	1) Remote Gateway 9100 Series unit ID
DISPLAYED TEXT	Attempt to recover to IP network failed to Remote Site: P1

Statistic	Definition
LOG NUMBER	42
DESCRIPTION	This log indicates that the IP network failed abruptly while there were connections routed over IP, dropping active voice calls. To check for dropped voice calls, look for log number 56.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Check if the IP connection is intact or if there is another problem on the IP network.
PARAMETERS	1) Remote Gateway 9100 Series unit ID
DISPLAYED TEXT	Abnormal failure of IP network. Remote Site: P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	43
DESCRIPTION	This log indicates the failure of a non-primary trunk. This might lead to dropping of voice calls to compensate the bandwidth loss in the absence of an IP connection to the Remote Gateway 9100 Series unit. Look for log number 56 to see if any calls were dropped.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	1) Verify that the PSTN connections are OK. 2) If this displays on the RLC, look for log number 46 on the Remote Gateway 9150 unit. If this ID is there, it is a genuine closure. 3) Link might have failed somewhere in the PSTN.
PARAMETERS	1) Remote Gateway 9100 Series unit ID
DISPLAYED TEXT	Abnormal failure of one of the additional trunks. Remote Site: P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	44
DESCRIPTION	This log indicates an abnormal failure of the primary signaling link. This leads to the dropping of all active connections to the Remote Gateway 9100 Series unit.
SEVERITY	CRITICAL
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check IP and trunk connections. (physical connections) 2) If this displays on the RLC, look for log number 45 on the Remote Gateway 9150 unit. If this log is there, it is a genuine closure. 3) Link might have failed some where in the Public network.
PARAMETERS	1) Remote Gateway 9100 Series unit ID to which communication is lost
DISPLAYED TEXT	Abnormal failure of primary signaling to Remote Site: P1
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	45
DESCRIPTION	This log indicates that the primary signaling was dropped due to a request for a 911 (emergency) call, resulting in a temporary loss of communication with RLC.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	This indicates that there are not enough trunks and the primary trunk had to be used for a 911 (emergency) call. Check if number of trunks can be increased (9150 only).
PARAMETERS	None
DISPLAYED TEXT	Primary trunk dropped to place 911 call

LOG NUMBER	46
DESCRIPTION	This log indicates that the system dropped one of the additional trunks to place a 911 (emergency) call as there were no available trunks.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Closing an additional trunk to place 911 call

Statistic	Definition
LOG NUMBER	47
DESCRIPTION	This log indicates that inactivity timer creation failed. This could lead to the primary signaling channel not closing to the remote. If the IP QoS is BAD, the PSTN trunk stays on. Otherwise, IP stay on.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	To overcome this situation, make sure no one is using a Remote Gateway 9100 Series unit telephone, then go to offline mode and come back to online. This restores normal operation. Use online/offline spree codes on the Remote Gateway 9150 or Remote Gateway 911x Series unit.
PARAMETERS	1) Remote Gateway 9100 Series unit ID
DISPLAYED TEXT	Timer creation failed. Signal will not be closed to Remote Site: P1

Statistic	Definition
LOG NUMBER	48
DESCRIPTION	This log indicates the failure of a connection because of incorrect security information due to one of the following situations: 1) A valid remote tried to connect with inappropriate security data. 2) The Remote Gateway 9100 Series unit rejected a connection initiated by the local unit. 3) There is a security issue with bringing up an additional trunk.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check that the security levels and security IDs are correct in configuration. 2) Security issue for additional trunks comes up if security level is CLID security and configuration is improper. 3) This may be an indication of an unauthorized Remote Gateway 9100 Series unit attempting to connect.
PARAMETERS	1) Remote Gateway 9100 Series unit ID 2) Medium 3) Connection type: primary/additional
DISPLAYED TEXT	Security Failure to Remote Site: P1 on Medium P2, ConnType = P3

Statistic	Definition
LOG NUMBER	49
DESCRIPTION	This log indicates that an unknown remote tried to connect and the attempt failed.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	<ol style="list-style-type: none"> 1) Confirm that the configuration of the unit IDs are OK between the units. 2) This may be an indication of an unauthorized Remote Gateway 9100 Series unit attempting to connect.
PARAMETERS	1) Unit ID of the Remote Gateway 9100 Series unit
DISPLAYED TEXT	Message from invalid Remote Site: P1
LOG NUMBER	50
DESCRIPTION	This log indicates that a connection came in on an unconfigured port and was rejected by the system. (PSTN connections)
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	<ol style="list-style-type: none"> 1) Check for proper port configurations on the RLC and Remote Gateway 9150 unit. 2) Check if a local call came in on a remote-only BRI port. Ensure that non-remote only BRI trunk numbers only are given to outsiders to call 9150's local sets. 3) Unauthorized unit may be trying to connect. Verify!
PARAMETERS	1) PSTN number from which the call originates
DISPLAYED TEXT	Incoming connection rejected. Address P1

Statistic	Definition
LOG NUMBER	51
DESCRIPTION	This log indicates that an incoming connection from the specified Remote Gateway 9100 Series unit failed because the specified medium is not allowed to connect to that Remote Gateway 9100 Series unit.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check the correctness of configurations. 2) Verify that unit trying to connect has needed authorization.
PARAMETERS	1) Unit ID of the Remote Gateway 9100 Series unit 2) The medium to which it attempted to connect
DISPLAYED TEXT	Remote Site: P1 trying to connect on unconfigured Medium P2]
LOG NUMBER	52
DESCRIPTION	This log indicates that no activity was found on the signaling link and all remote service phones were idle.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Remote Gateway 9100 Series unit ID
DISPLAYED TEXT	Signaling closed to Remote Site: P1 due to no activity

Statistic	Definition
LOG NUMBER	53
DESCRIPTION	This log indicates that the Remote Gateway 9100 Series unit went offline. No communication is possible until the unit goes online again or online time occurs. In offline mode, all connections, including permanent trunks, if any, are closed.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Remote Gateway 9100 Series unit ID going offline
DISPLAYED TEXT	Close signal as unit goes offline. Remote Site: P1
LOG NUMBER	54
DESCRIPTION	This log indicates an attempt to reach an invalid remote.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for proper configuration 2) Check for updates completed while system was active. 3) If the message is consistent, even after proper configuration, report to vendor.
PARAMETERS	1) Unit ID of Remote Gateway 9100 Series unit to which connection was attempted
DISPLAYED TEXT	Connection attempted to invalid Remote Site: P1

Statistic	Definition
LOG NUMBER	55
DESCRIPTION	<p>This log indicates the system was unable to place a voice call, which could be caused by the following conditions:</p> <ol style="list-style-type: none"> 1) No connection to the remote. Attempts failed. 2) HIGH/NORMAL priority: No bandwidth on trunk and IP not available. 3) PSTN only call: No bandwidth available, trunk disabled, or trunk not reachable. 4) IP only call: IP not reachable or not enabled. 5) Some inconsistency within the system - Synchronization between RLC - 9150/911x.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	<ol style="list-style-type: none"> 1) Verify correctness of configurations. 2) Verify physical connections on the medium according to information in 1), above. <p>Note: If this happens consistently for all calls, and is not an obvious problem due to configuration or bandwidth limitations, view the statistics and report the problem.</p>
PARAMETERS	<ol style="list-style-type: none"> 1) Remote Gateway 9100 Series unit ID 2) amount of bandwidth the system needs to place the additional call
DISPLAYED TEXT	Voice call did not succeed to Remote Site: P1 [BW required P2]

Statistic	Definition
LOG NUMBER	56
DESCRIPTION	This log indicates an abnormal failure of a call. Possible reasons include: 1) Sudden link failure on the given medium 2) Drop of remote trunks on the 9150/911x side for a 911 (emergency) call 3) Sudden primary signaling failure
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Look for log numbers 42, 43, and 44 to ascertain the reason active calls were dropped.
PARAMETERS	1) Bandwidth of the call 2) Unit ID of remote to which call is connected 3) Medium on which the call was active at the time of failure
DISPLAYED TEXT	Call of P1 BW got dropped to Remote Site: P2, medium: P3
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	57
DESCRIPTION	This log indicates a failed attempt to switch a voice connection to the specified medium. This is an indication of a loss of one of the following: 1) Signaling packets 2) Synchronization between RLC - 9150, 911x
SEVERITY	MINOR
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	This does not happen in normal operation. Report its occurrence.
PARAMETERS	1) Bandwidth of the call 2) Medium from which the system attempted to switch the call 3) Medium to which the system attempted to switch the call 4) Remote Gateway 9100 Series unit ID
DISPLAYED TEXT	Call of P1 BW did not switch from medium: P2 to medium: P3 Remote Site: P4
LOG NUMBER	58
DESCRIPTION	This log indicates that there is no available trunk in the given trunk group to place a local trunk call.
SEVERITY	MINOR
TASK	Network Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	If this happens consistently, consider reconfiguring B-channel allocations on the Remote Gateway 9150 unit.
PARAMETERS	1) Trunk Group Number
DISPLAYED TEXT	Local call did not succeed

Statistic	Definition
LOG NUMBER	59
DESCRIPTION	This log indicates that a local call was dropped because of an abnormal link failure.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	1) Confirm that physical trunk connections are intact. 2) Check for failure on the PSTN.
PARAMETERS	None
DISPLAYED TEXT	Local trunk call abnormally failed

LOG NUMBER	60
DESCRIPTION	This log indicates that a local trunk call was dropped for an emergency (911) call because there were no free trunks.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Local call dropped for 911

Statistic	Definition
LOG NUMBER	61
DESCRIPTION	This log indicates that the signaling link to a Remote Gateway 9100 Series unit was established on the specified medium.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Remote Gateway 9100 Series unit ID 2) Medium
DISPLAYED TEXT	Signaling is UP to Remote Site: P1 on medium: P2
LOG NUMBER	62
DESCRIPTION	This log indicates that the IDVR server has gone down. (This log is not generated in the 1.2.1 release.)
SEVERITY	MAJOR
TASK	Device Control, Call Processing
PRODUCT	RLC, 9150, IDVR
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for the IP connectivity to server. 2) Check for the IDVR server status.
PARAMETERS	1) IDVR server's IP address
DISPLAYED TEXT	IDVR server status: P1

Statistic	Definition
LOG NUMBER	63
DESCRIPTION	<p>This log indicates a PSTN connection to a peer unit failed. This could be caused by several possible problems, including:</p> <ol style="list-style-type: none">1) A cabling issue at the Remote Gateway 9100 Series unit could keep that unit from being able to connect on the PSTN.2) The data port on the RLC could be disabled.3) For BRI connections between a 9150 and an RLC the PSTN path may not be a 64K clear channel (the required path).4) Incorrect dial numbers could be keeping the circuit from establishing.5) Bit errors could be occurring preventing communication from working. This could be due to bad cables or a bad connection.
SEVERITY	MAJOR
TASK	TP
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	<p>To check for the possible problems named above, do the following:</p> <ol style="list-style-type: none">1) Check the PSTN connections at the Remote Gateway 9100 Series unit.2) Confirm that the RLC's data port is enabled.3) Confirm that BRI connections between a 9150 unit and its RLC are 64K clear channel (the required path).4) Confirm that the correct numbers are configured on both ends.5) Confirm that cables and connections on both ends are good.
PARAMETERS	None
DISPLAYED TEXT	PSTN connection failed to initialize

Statistic	Definition
LOG NUMBER	64
DESCRIPTION	This log indicates that the unit attempted a PSTN connection to its peer unit at too slow a bit rate. This severely damages system performance since all bandwidth calculations are incorrect.
SEVERITY	MAJOR
TASK	TP
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	<p>The PSTN path between a 9150 and RLC requires a clear 64K channel.</p> <p>If this log occurs every time a PSTN call is made, then either the wrong service has been ordered from the telephone company or the telephone company has provided the wrong service.</p> <p>If this log occurs intermittently then the connection through the central office has encountered some sort of problem.</p> <p>It is still possible, however, that the wrong service has been ordered, or provided, and that the majority of the time the PSTN has had a clear channel by chance. Some customers have reported that they requested the 64K channel, but a 54K channel was provided instead.</p> <p>Another possible scenario is that bit errors could be occurring, preventing communication from initializing at 64K, but allowing 56K. This is probably the least frequent cause.</p>
PARAMETERS	None
DISPLAYED TEXT	PSTN connection initialized at 56K clear channel unavailable

Statistic	Definition
LOG NUMBER	65
DESCRIPTION	This log indicates that the unit attempted a PSTN connection to its peer unit, and that the connection attempt succeeded initially at 56K, failed at 65K, and then failed again at 56K.
SEVERITY	MAJOR
TASK	TP
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN:	<p>This problem is most likely related to log number 64 where a clear 64K channel could not be obtained.</p> <p>It is possible that the attempt to increase speed to 64K caused a problem with the central office, making it impossible to re-establish at 56K. This would increase the likelihood of the problem being due to a high bit error rate on the link.</p>
PARAMETERS	None
DISPLAYED TEXT	PSTN connection failed to re-initiate at 56K

Statistic	Definition
LOG NUMBER	66
DESCRIPTION	This log indicates that the database has been converted from an older version to the current version. The start and end versions are specified. The status of the conversion is also available.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	If the status is Failure, then re-configure the system.
PARAMETERS	1) Status 2) Starting version (From version) 3) Current version (To version)
DISPLAYED TEXT	Database Conversion: P1 P1 [From Ver P2 to P3]

Statistic	Definition
LOG NUMBER	67
DESCRIPTION	This log indicates that a locally defined feature clashes with a PBX defined feature.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN:	1) In the case of failure, check the key configurations on the switch and the key configurations done on the 911x, 9150, IDVR for the port concerned. 2) In case of clash re-define the local feature on a key that is not being used for a PBX feature.
PARAMETERS	1) Remote Gateway 9100 Series unit Port Number 2) Key Number
DISPLAYED TEXT	Port P1: Local Feature Overrides PBX Feature on key P2

Statistic	Definition
LOG NUMBER	68
DESCRIPTION	This log indicates that a PSTN connectivity test has started to a specified remote, in a specified mode.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	1) Remote board ID 2) Mode in which test started a) Disruptive test b) Non disruptive test
DISPLAYED TEXT	PSTN connectivity test started for remote = P1, in mode = P2

Statistic	Definition
LOG NUMBER	69
DESCRIPTION	This log indicates that a PSTN connectivity test is completed or aborted.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	1) Remote board ID 2) Reason that the test ended a) Normal end b) Aborted
DISPLAYED TEXT	PSTN connectivity test ended for remote = P1 and P2

Statistic	Definition
LOG NUMBER	70
DESCRIPTION	This log indicates that there was a failure in adding a DN to the system because the DN was already in the system. If you want to place a local call to this digital telephone set, you must use the number configured through Configuration Manager.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	Do not configure MADN on the primary key if both of the digital telephone sets are on the Remote Gateway 9150 unit.
PARAMETERS	1) Remote Gateway 9100 Series unit Port Number 2) DN which couldn't be added to the system
DISPLAYED TEXT	MADN Conflict for DN P1 on Port P2: Could not update local DN

Statistic	Definition
LOG NUMBER	71
DESCRIPTION	<p>This log indicates that the PBX has returned an Illegal number error when attempting to dial from the Network port on the RLC to the Remote Gateway 9150 unit.</p> <p>Most frequently, this error occurs when the dialed number is going to be routed by the PBX, or Central Office, over an analog trunk instead of a clear channel data path.</p>
SEVERITY	MAJOR
TASK	DL
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	<ol style="list-style-type: none"> 1) Verify that the Network port is configured correctly on the PBX. 2) Verify that the number dialed from the RLC to the Remote Gateway 9150 unit is correct. 3) Verify that the PBX trunks used allow clear channel data. LD 80 traces of the data port are helpful. 4) Verify that Central Office is not routing the data call over voice circuits.
PARAMETERS	<ol style="list-style-type: none"> 1) Network port from which this call was placed 2) Last number dialed by a Network port, usually this port
DISPLAYED TEXT	Network Port P1 call to P2 may be routed over Voice circuits

Statistic	Definition
LOG NUMBER	72
DESCRIPTION	This log indicates that a key map update is written into the Flash.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	1) Status - SUCCESS if Save to Flash is successful. FAILED if the Flash save attempt failed.
DISPLAYED TEXT	Key Map Save to Flash: P1
LOG NUMBER	73
DESCRIPTION	This log indicates an invalid compression algorithm (such as, G.729A/Fax or G.726) has been configured for a port connected to a Remote Gateway 911x Series unit and that the algorithm has been reset to G.729A.
SEVERITY	WARNING
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	1) Unit ID of the 911x unit 2) Port number used for the 911x unit
DISPLAYED TEXT	"Remote Site: P1[911x] registered to Port P2 with Invalid Compression, reset to G.729A

Statistic	Definition
LOG NUMBER	74
DESCRIPTION	This log indicates a status change (such as, UP/DOWN) for the BRI line.
SEVERITY	WARNING
TASK	BRI Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	1) Describes status change (such as, UP/DOWN) 2) BRI Module Number
DISPLAYED TEXT	P1 detected for BRI Module P2
PRODUCES HOST PBX ALARM AND ALERT	Yes
LOG NUMBER	75
DESCRIPTION	This log indicates that the system is not able to bring up an analog line due to non-availability of modem DSPs.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	1) Ensure that enough Modem channels are configured on the DSPs. 2) Determine whether you need more DSP application modules to provide adequate DSP resources.
PARAMETERS	1) Unit ID of the affected remote unit
DISPLAYED TEXT	Not able to connect remote: P1 on modem due to non availability of Modem channels

Statistic	Definition
LOG NUMBER	76
DESCRIPTION	This log indicates that the software version of the remote unit is incompatible with the software version installed in the unit generating this message.
SEVERITY	CRITICAL
TASK	Network Manager
PRODUCT	9150, RLC, 911x
CANCELLATION	None
ACTION TO BE TAKEN:	Verify software versions on both units.
PARAMETERS	1) Remote Unit ID
DISPLAYED TEXT	Communication with Remote P1 is not possible due to software incompatibility
PRODUCES HOST PBX ALARM AND ALERT	Yes
LOG NUMBER	77
DESCRIPTION	This log indicates that the RLC's remote unit configuration does not match the remote device that is initiating the call. This is probably due to a configuration error.
SEVERITY	CRITICAL
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	A log that indicates signaling is up on any medium to that remote unit.
ACTION TO BE TAKEN:	1) Verify the Remote Unit configuration. 2) Ensure that no one else is trying connect to this unit through improper configuration.
PARAMETERS	1) Remote Unit ID
DISPLAYED TEXT	Remote Unit = P1 is found to be of incompatible board type. Communication not possible

Statistic	Definition
LOG NUMBER	78
DESCRIPTION	This log indicates that the key map version of the PBX software has changed. This is normal when upgrading major PBX versions.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	1) Key map database start version 2) Key map database end version 3) Status (Success or Failure)
DISPLAYED TEXT	PBX Model database conversion from Ver P1 to Ver P2 P3
LOG NUMBER	79
DESCRIPTION	This log indicates an error in reading key map Flash.
SEVERITY	MAJOR
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN:	1) Reset remote unit. If the problem persists, try action #2. 2) Disable and re-enable the RLC. If the problem persists, try action #3. 3) Reset the RLC and the remote unit. If the problem persists, contact your vendor.
PARAMETERS	1) SUCCESS or reason for failure
DISPLAYED TEXT	PBX Model database read - P1

Statistic	Definition
LOG NUMBER	80
DESCRIPTION	This log indicates that connectivity on the specified medium to the specified remote unit closed. This is a part of normal system operation.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Remote unit 2) Medium (ISDN, IP)
DISPLAYED TEXT	Connectivity is closed to Remote: P1 on Medium: P2

Statistic	Definition
LOG NUMBER	81
DESCRIPTION	This log indicates that connectivity on the specified medium to the specified remote failed abnormally due to an unspecified problem on the network.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	A message that indicates that signaling is up on the specified medium
ACTION TO BE TAKEN	Check for the following on the specified medium: 1) Check the network connectivity both at the RLC and remote site. 2) Check if any problem arose anywhere else on the network between the RLC and remote site. 3) Check if any of the units were reset for any reason.
PARAMETERS	1) Remote unit 2) Medium (ISDN, IP)
DISPLAYED TEXT	Abnormal failure of connectivity on Medium: P1 to Remote: P2
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	82
DESCRIPTION	<p>This log indicates that Network Manager task states for a particular remote unit was reset and all the connections to the remote were cleared. This can happen due to the following reasons:</p> <ol style="list-style-type: none">1) An error occurred in the system to automatically trigger Network Manager reset.2) The user has issued a debug command "nmr x" where x is a valid remote unit number.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	<p>System usually works as normal after the log is displayed. If not, contact technical support personal for help. If the log is displayed too frequently, check if anyone is entering debug commands. If not, contact technical support.</p>
PARAMETERS	1) Remote unit
DISPLAYED TEXT	States reset in NM for Remote: P1

Statistic	Definition
LOG NUMBER	83
DESCRIPTION	This log indicates the result of DN Discovery on the RLC. If the result in the log is Failure or Partial Success then the system retries for up to five times at three minute intervals if the port(s) is (are) busy during the first attempt. The system records the status of the initial attempt as well as the last attempt, if made.
SEVERITY	NORMAL
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	Ensure that the log shows SUCCESS after every DN Discovery session (either triggered by time-of-day or manually). In case of FAILURE/PARTIAL SUCCESS, check if the DN Discovery port is in idle (not in set busy or call forwarded) state.
PARAMETERS	1) Status: SUCCESS, PARTIAL SUCCESS, FAILURE
DISPLAYED TEXT	DN Discovery has completed: result - P1

Statistic	Definition
LOG NUMBER	84
DESCRIPTION	This log indicates that a voice/modem DSP has loaded successfully.
SEVERITY	NORMAL
TASK	VPM
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Single-digit DSP device ID 2) DSP module 3) DSP device
DISPLAYED TEXT	DSP #P1 load successful. (P2, P3)

Statistic	Definition
LOG NUMBER	85
DESCRIPTION	<p>This log indicates that a voice/modem DSP load attempt has Failed, indicating a possible hardware problem.</p> <p>If this log entry is not followed by log entry 83, the DSP is out of service for the duration of the session (that is, until RESET or power-cycle).</p> <p>On the 911x, this message indicates failure of the only DSP and represents a CRITICAL failure.</p>
SEVERITY	MAJOR (CRITICAL on 911x)
TASK	VPM
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 83 (DSP load successful)
ACTION TO BE TAKEN	<p>1) Swap DSP module slot positions to see if the failure follows one DSP module. Report failures to on-board DSPs (Module 0) to Nortel.</p> <p>2) Check DSP status using Configuration Manager's Alarms/Stats/Logs → DSP Statistics screen.</p>
PARAMETERS	<p>1) Single-digit DSP device ID</p> <p>2) DSP module number</p> <p>2) DSP device number</p>
DISPLAYED TEXT	DSP #P1 load failure. (P2, P3)
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	86
DESCRIPTION	This log indicates that a DSP failure was detected and automatic dynamic recovery was initiated.
SEVERITY	WARNING
TASK	VPM
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	<p>1) Single-digit DSP device ID</p> <p>2) DSP module number</p> <p>3) DSP device number</p> <p>4) If the user manually initiates the request, the cause shows as User. If the reload arose from detection of DSP failure and subsequent automatic dynamic DSP recovery, the cause shows as Auto.</p> <p>Note: If the DSP has already been taken out of service (OOS) due to catastrophic failure, the code ignores the reload request and leaves the DSP OOS.</p>
DISPLAYED TEXT	DSP #P1 reloading. (Mod, Dev) = (P2, P3) Cause: P4

Statistic	Definition
LOG NUMBER	87
DESCRIPTION	This log indicates that a DSP has been taken Out Of Service. This can occur for the following reasons: 1) Download or initialization failure (such as, at system startup) 2) Dynamic DSP failure with automatic recovery 3) User execution of the DSP restart debug command, which first takes the DSP OOS, then tries to restart it
SEVERITY	MAJOR (CRITICAL on 911x)
TASK	VPM
PRODUCT	RLC, 9150, 911x
CANCELLATION	This action is followed by either log number 83 or 84, to indicate reload SUCCESS or FAILURE, respectively.
ACTION TO BE TAKEN	No action is required unless this results from DSP load failure (refer to log number 84).
PARAMETERS	1) Single-digit DSP device ID 2) DSP module number 3) DSP device number
DISPLAYED TEXT	DSP #P1 taken OOS. (Module, Device) = (P2, P3)
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	88
DESCRIPTION	This log indicates that a modem channel has been requested when no modem channels were available. It can occur if an insufficient number of DSPs have been configured with the 911x DSP load.
SEVERITY	MAJOR (CRITICAL on 911x)
TASK	VPM
PRODUCT	RLC, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Check the RLC configuration to ensure that a sufficient number of DSPs have been configured with the 911x DSP load.
PARAMETERS	None
DISPLAYED TEXT	Modem channel request denied: No modem channels available
LOG NUMBER	90
DESCRIPTION	This log indicates that no emergency number is programmed in the table..
SEVERITY	NORMAL
TASK	MMI
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN:	Configure at least one emergency number on the Remote Gateway 9100 Series Configuration Manager 9150 or 911x System Configuration property sheet, as appropriate to your remote unit.
PARAMETERS	None
DISPLAYED TEXT	No Emergency no's are configured

Statistic	Definition
LOG NUMBER	91
DESCRIPTION	This log indicates the status of a BRI module that has started (or restarted) because of a system startup or manual restart.
SEVERITY	WARNING
TASK	BRI manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	<p>Monitor the BRI module. If the cause is not a user-initiated reset, a problem exists with either the BRI hardware or software. Try replacing the BRI module, or swapping the BRI module with another slot that shows no problem. If the problem persists, contact Nortel.</p> <p>Note: MMI code (via MMI_SW_UPLD_LOG_ID) reports the status of a BRI module restart resulting from an upload command.</p>
PARAMETERS	<p>1) BRI Module</p> <p>2) Reset status (SUCCESS or FAILURE), activity leading to the error (System Startup, User Reset)</p>
DISPLAYED TEXT	BRI #P1 boot status: P2

Statistic	Definition
LOG NUMBER	92
DESCRIPTION	This log indicates that there is a mismatch in the circuit rule for the MADN ports. All ports in the same MADN group should have the same compression rate and priority.
SEVERITY	WARNING
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	Configure the Circuit rule for all the ports in the MADN Group the same. Save the configuration and force DN Discovery from Configuration Manager.
PARAMETERS	1) MADN Group Number 2) DN 3) Port Number 4) Port Number
DISPLAYED TEXT	MADN group P1 (DN P2) Circuit rule mismatch for ports P3 and P4

Statistic	Definition
LOG NUMBER	93
DESCRIPTION	This log indicates that the Emergency Access Code (EAC) has been dialed from a port.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Port number that dialed the emergency access code 2) DN that dialed the emergency access code
DISPLAYED TEXT	Emergency Code Dialed from port: P1, DN: P2
PRODUCES HOST PBX ALARM AND ALERT	Yes
LOG NUMBER	94
DESCRIPTION	This log indicates that ONLINE SPRE code was dialed from a port.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 2 - FB_RECOVERY_LOG_ID
ACTION TO BE TAKEN	None
PARAMETERS	1) Port number that dialed the SPRE code
DISPLAYED TEXT	Online SPRE Code dialed from port: P1

Statistic	Definition
LOG NUMBER	95
DESCRIPTION	This log indicates that the OFFLINE SPRE code was dialed from a port.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 2 - FB_RECOVERY_LOG_ID
ACTION TO BE TAKEN	None
PARAMETERS	1) Port number that dialed the SPRE code
DISPLAYED TEXT	Offline SPRE Code dialed from port: P1
LOG NUMBER	96
DESCRIPTION	This log indicates that the Auto Upgrade function was attempted.
SEVERITY	NORMAL
TASK	Auto Upgrade
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 2 - FB_RECOVERY_LOG_ID
ACTION TO BE TAKEN	None
PARAMETERS	1) Success/Failed 2) TCPIP Address of TFTP Server used 3) Filename used in the transfer 4) Result of the action
DISPLAYED TEXT	Upgrade P1 TFTP Server: P2 File: P3 - P4
PRODUCES HOST PBX ALARM AND ALERT	Yes

Statistic	Definition
LOG NUMBER	97
DESCRIPTION	This log indicates that no activity is found on the signaling link, when all digital telephone sets connected to Remote Gateway 911x Series units are idle, and the modem needs to be retrained. The error is detected by the RLC.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Remote Unit ID
DISPLAYED TEXT	Modem retrain, remote ID P1, error detected by RLC
LOG NUMBER	99
DESCRIPTION	This message indicates that an incoming call is being transferred due to network congestion but the transfer has failed.
SEVERITY	CRITICAL
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	Check PBX configuration.
PARAMETERS	1) String indicating the nature of the failure. 2) Destination port number of the incoming call. 3) Device key number the call is on.
DISPLAYED TEXT	Network Congestion Call Transfer failure: P1 Port P2, Key P3

Statistic	Definition
LOG NUMBER	100
DESCRIPTION	This message indicates that an incoming call is being transferred due to network Congestion but the transfer has failed.
SEVERITY	MAJOR
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	Check PBX configuration for this device.
PARAMETERS	1) String indicating the nature of the failure. 2) Destination port number of the incoming call. 3) Device key number the call is on.
DISPLAYED TEXT	Network Congestion Call Transfer failure: P1 Port P2, Key P3
LOG NUMBER	101
DESCRIPTION	This message indicates that an incoming call is being transferred due to network congestion but the transfer has failed.
SEVERITY	MINOR
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	Check communication with the PBX.
PARAMETERS	1) String indicating the nature of the failure. 2) Destination port number of the incoming call. 3) Device key number the call is on.
DISPLAYED TEXT	Network Congestion Call Transfer failure: P1 Port P2, Key P3

Statistic	Definition
LOG NUMBER	102
DESCRIPTION	This message indicates successful transfer of an incoming call due to network congestion.
SEVERITY	NORMAL
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) String indicating "Completed". 2) Destination port number of the incoming call. 3) Device key number the call is on.
DISPLAYED TEXT	Network Congestion Call Transfer: P1 Port P2, Key P3
LOG NUMBER	103
DESCRIPTION	Indication of the PSTN Direction Establishment feature.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) String
DISPLAYED TEXT	PSTN Direction Establishment Feature P1.

Statistic	Definition
LOG NUMBER	104
DESCRIPTION	Software system reset is being performed.
SEVERITY	NORMAL
TASK	None
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Software System Reset.

Glossary

10BaseT Ethernet

The Ethernet standard for baseband local area networks using twisted-pair cable carrying 10 megabits per second (Mbps) in a star topology.

A

A-law

A companding technique used in encoding and decoding audio signals in 30-channel pulse code modulated (PCM) systems. A-law companding is the primary method used in Europe. *Refer also to* Mu-law.

adapter

Hardware required to support a particular device. For example, network adapters provide a port for the network wire. Adapters can be expansion boards or part of the computer's main circuitry.

administrator

A user who is responsible for maintaining the RLC or its associated remote units.

agent

A person who is responsible for handling customer calls.

analog

The type of signal used by most telephone connections. A modem converts a digital (computer) signal to analog, and vice versa, so that the signal can travel through telephone lines.

API

Refer to Application Program Interface.

application

A program that runs on a computer.

Application Program Interface

A set of routines, protocols, and tools that programmers use to develop software applications. APIs simplify the development process by providing commonly used programming procedures.

Automatic Call Distribution (ACD) applications

A separate system or built-in feature of a PBX that equally distributes incoming calls to agents. As calls come in, they are placed into a queue (or a waiting line) for the next available agent. The RLC and its associated remote units support all of Nortel's ACD applications.

B**bandwidth**

The amount of data that the network can transmit, usually expressed in Mbytes per second.

baseboard

Refer to motherboard.

Basic Input/Output System

Flash ROM-based code that runs the Power-On Self-Test (POST) and bootstrap loader. BIOS contains low-level access routines for hardware that can be called from DOS.

BIOS

Refer to Basic Input/Output System.

bit

Short for binary digit, the smallest unit of information on a machine. A single bit can hold only one of two values: 0 or 1.

branch station

A telephone set or fax machine located at the Remote Gateway 9150 site.

BRI

Basic Rate Interface. An ISDN subscriber service that uses two B (64 Kbps) channels and one D (64 Kbps) channel to transmit voice, video, and data signals.

bridge

A protocol-independent device that connects two LANs or two segments of the same LAN. Bridges are faster (and less versatile) than routers because they forward packets without analyzing and rerouting messages.

bus

A collection of wires that connects the microprocessor and main memory to internal computer components. All buses consist of an address bus that transfers data and a data bus that transfers information about where the data should go.

In a network, the bus (also called the backbone) is the main cable that connects all devices on a LAN.

byte

Abbreviation for binary term, a unit of storage capable of holding a single character. On almost all modern computers, a byte is equal to eight bits. Large amounts of memory are indicated in terms of kilobytes (1024 bytes), megabytes (1 048 576 bytes), and gigabytes (1 073 741 824 bytes).

C**cache**

A temporary storage area in computer memory.

call duration timer

Used in PSTN mode only, it specifies the minimum length of time that each call to the host PBX remains open, regardless of telephone activity (or lack thereof).

call on demand

A call connection that is opened only when a connection to the host PBX is required. This is different from a permanent connection, which is open all the time.

call treatment

A method of handling applied to a call while it is waiting to be answered or serviced.

Caller ID

Caller ID is used on the RLC to identify the number of the caller requesting access to one of its ports. It is also used on the Remote Gateway 9150 unit to authenticate incoming calls from the RLC.

Calling Line Identification

An optional service that identifies the telephone number of the caller. This information can then be used to route the call to the appropriate agent or skillset. The caller's telephone number can also be displayed on a telephone set.

card

A thin, rectangular plate on which chips and other electronic components are placed. Examples of cards include motherboards, expansion boards, daughterboards, controller boards, network interface cards, and video adapters.

CD-ROM

A type of optical disk capable of storing large amounts of data (up to 1 Gbyte), although the most common size is 630 Mbytes. A single CD-ROM has the storage capacity of 700 floppy disks and is particularly well-suited to information that requires large storage capacity.

CLAN

Refer to Customer Local Area Network.

CLID

Refer to Calling Line Identification.

client

The part of a client/server architecture that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

codec

An acronym for COder-DECoder. A device that codes analog signals into digital signals for transmission and decodes digital signals into analog signals for receiving.

COM or COMM

Communications port. This usually refers to the Logical Device name of PC serial ports as defined by DOS.

computer-based training

Computer-based training (CBT) is a type of education in which students learn by running special training programs on a computer. CBT is especially effective for training people to use computer applications, because the CBT program can be integrated with the applications.

Configuration Manager

The software application used to configure and administer the Remote Gateway 9150 unit and the RLC to which it is connected.

controller board

A special type of expansion board that contains a controller for a peripheral device. When you attach new devices to a computer, such as a disk drive, often a controller board must also be added.

CPU

Central Processing Unit. This is the system unit that holds a PC's essential components.

crash

A serious computer failure during which the computer stops working or a program closes unexpectedly. A crash indicates a hardware malfunction or a serious software bug.

Customer Local Area Network

The LAN to which your corporate services and resources connect. The RLC and its associated remote units both connect to the CLAN.

D**daughterboard**

Usually used as a synonym for an expansion board, a daughterboard is any printed circuit board that connects directly or indirectly to a motherboard.

DB-9 connector

A 9-pin connector labeled ADMIN that provides the RS-232 serial port interface. This serial port connection can be used to configure a Remote Gateway 9150 unit that is directly connected to a PC.

DHCP

Refer to Dynamic Host Configuration Protocol.

Digital Signal Processor

A special type of coprocessor that manipulates analog data, such as sound or photographs, that has been converted to digital form.

Directory Number

The number that identifies a phoneset on a switch. The directory number (DN) could be a local extension (local DN), a public network telephone number, or an automatic call distribution directory number (ACD-DN).

DLL

Refer to Dynamic Link Library.

DN

Refer to Directory Number.

driver

A program that controls a device. Every device, whether it is a printer, disk drive, or keyboard, must have a driver program. A driver acts like a translator between the device and programs that use the device.

DSP

Refer to Digital Signal Processor.

Dynamic Host Configuration Protocol

A protocol for dynamically assigning IP addresses to devices on a network.

Dynamic Link Library

A library of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions and a program accesses the functions by creating either a static or dynamic link to the DLL. A DLL can be used by several applications at the same time.

dynamic port pool

A RLC feature that is similar to multi-user ports in that multiple stations can share ports on the RLC. However, users sharing ports from a dynamic pool are assigned to the first available port on the RLC.

E**ECC**

Refer to Error Correction Code.

EEPROM

Refer to Electronically Erasable Programmable Read-Only Media.

ELAN

Refer to Embedded Local Area Network.

Electronically Erasable Programmable Read-Only Media

A memory chip that needs only a higher than normal voltage and current to erase its contents. An EEPROM chip can be erased and reprogrammed without taking it out of its socket. An EEPROM chip gives a computer and its peripherals a means of storing data without the need for a constant supply of electricity.

Embedded Local Area Network

This is the network connection from the PBX to the RLC. It is an Ethernet LAN that is segmented from the rest of the Ethernet network and enables signaling and administration access to the RLC. Nortel recommends the following:

- IP traffic should not be routed between the main network and the ELAN.
- An IP route should not be established between the two LANs.

Emergency Service Number

The Remote Gateway 9150 unit allows you to program an emergency service number (such as 911).

EMI

Electromagnetic Interference

Error Correction Code

A scheme that can detect and fix single-bit memory errors without crashing the system. Also known as Error Detection and Correction (EDAC).

Ethernet

A widely used LAN protocol that uses a bus topology and supports data transfer rates of 10 Mbps.

event

An occurrence or action on the RLC or remote unit, such as the sending or receiving of a message, the opening or closing of an application, or the reporting of an error. Some events are for information only, while others can indicate a problem.

expansion board

Any board that plugs in to one of the computer's expansion slots. Expansion boards include controller boards, LAN cards, and video adapters.

expansion bus

Enables expansion boards to access the microprocessor and memory. *Refer to also* bus.

F**first-level threshold**

The value that represents the lowest value of the normal range for a given field in a threshold class. The system tracks how often the value for the field falls below this value.

G

G.711

G.711 is the international standard for encoding telephone audio on a 64 Kbps channel. It is a pulse code modulation (PCM) scheme operating at an 8 kHz sample rate, with 8 bits per sample. According to the Nyquist theorem, which states that a signal must be sampled at twice its highest frequency component, G.711 can encode frequencies between 0 and 4 kHz. Telephone companies can select between two different variants of G.711: A-law and μ -law. A-law is the standard for international circuits.

G.726

G.726 is a standard ADPCM algorithm specified by the International Telecommunication Union (ITU) for reducing the 64 kbps A-Law or μ -law logarithmic data of a normal telephone line to 16, 24, 32, or 40 kbps.

G.729A

G.729A is a voice compression International Telecommunications Union (ITU) standard that can be used in a wide range of applications including wireless communications, digital satellite systems, packetized speech, and digital leased lines. G.729A provides 8 Kbps of bandwidth for compressed speech at toll quality (equivalent to G.726 32 Kbps ADPCM under clean channel condition).

gateway

A device that functions as a node on two or more networks, forwarding packets from one network to addresses in the other networks. In Remote Gateway 9100 Series context, the gateway is the device on the network that directs traffic to and from the Remote Gateway 9150 unit or RLC.

Gigabyte (Gbyte)

1 073 741 824 bytes. One Gbyte is equal to 1024 Mbytes.

General Protection Fault

A computer condition that causes a Windows application to crash. GPFs usually occur when one application attempts to use memory assigned to another application.

GPCP

General Purpose Computing Platform

GPF

Refer to General Protection Fault.

graphical user interface

The information displayed on the monitor when a Windows application (or another non-command-based application) runs. A graphical user interface uses features such as pointers, icons, I-beams, and menus to make the program easier to use.

H**handshaking**

A process involved in establishing a valid connection or signal between two pieces of hardware or communications software.

host call appearance key

An assigned key on the telephone set at the remote site that is used to establish a connection with the host PBX or to receive incoming calls from the host PBX.

host-controlled call mode

When a call is placed to someone at the host site, or when someone from the host site calls the remote site, the call is in host-controlled call mode. Calls in host-controlled mode are routed through the PBX.

host station

A telephone set located at the host PBX site.

host trunk

The ISDN PRI or TI connection located at the host site. Host trunks are used to route calls from the host PBX to remote sites over the PSTN.

hub

A common connection point for all 10Base-T cables connected to a small network. A hub enables data to go from one device to another.

I**icon**

A small picture that represents an object or program in a graphical user interface.

idle timer

Identifies the maximum length of time during which an ISDN connection should remain idle before it can be closed. Idle means that a voice connection does not exist, and buttons are not being pressed on the digital telephone.

input/output

Refers to any operation, program, or device that enters data into a computer or extracts data from a computer.

I/O

Refer to input/output.

IP

Internet Protocol. The protocol within TCP/IP that governs the breakup of data messages into packets, the routing of the packets from sender to destination network, and the reassembly of the packets into the original data messages at the destination.

IP address

Internet Protocol address. An identifier for a computer or device on a TCP/IP network. Networks use the TCP/IP protocol to route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0–255. For example, 1.160.10.240 can be an IP address.

ISDN

Integrated Services Digital Network. A worldwide digital communication protocol that permits telephone networks to carry data, voice, and other source material. There are two kinds of ISDN lines—Primary Rate Interface (PRI) and Basic Rate Interface (BRI). *Refer also to* BRI.

J**jumper**

A metal bridge that closes an electrical circuit. Typically, a jumper consists of a plastic plug that fits over a pair of protruding pins. Jumpers are sometimes used to configure expansion boards. By placing a jumper plug over a different set of pins, you can change a board's parameters.

K

kilobyte (kbyte)

1024 bytes

L

LAN

Refer to Local area network.

LED

Light emitting diode

Local area network

A computer network that spans a relatively small area. Most LANs connect workstations and personal computers and are confined to a single building or group of buildings.

local call

A call that originates at your site.

local call appearance key

An assigned key on the telephone set at the Remote Gateway 9150 site that is used to call another station at the branch office, or to place and receive calls through the local PSTN.

locally controlled call mode

When you place a call from a specified local call appearance key, or your call is to another telephone at your branch site, you are in locally controlled call mode. Calls in locally controlled mode are routed through the local PSTN.

local station

A telephone set located at the Remote Gateway 9150 site.

M

M1

Meridian 1 PBX

Megabyte (Mbyte)

1 048 576 bytes

megahertz (MHz)

One million cycles per second.

RLC

An abbreviation for Reach Line Card. The RLC is installed on the host PBX at the host location and relays voice and signaling information from the digital telephones connected at a remote site to the PBX at the host site.

motherboard

The principal board that has connectors for attaching devices to the bus. Typically, the motherboard contains the CPU, memory, and basic controllers for the system. On PCs, the motherboard is often called the system board.

MTBF

Mean time between failures

Mu-law

A companding method for encoding and decoding audio signals in 24-channel pulse-code-modulated (PCM) systems. Mu-law is the method used in North America and Japan. *Refer also to A-law.*

Multi-user ports

A RLC port feature that allows multiple stations to time-share a single port on the host PBX. All stations that use a multi-user port are always assigned to the same port number (TN) on the host PBX.

N

network interface card

An expansion board that enables a PC to be connected to a local area network (LAN).

NIC

Refer to network interface card.

node

A device connected to the network capable of connecting to other network devices. For example, the RLC and Remote Gateway 9150 unit are both nodes on the network.

NPA

Refer to Number Plan Area.

Number Plan Area

Area code

NVRAM

Non-Volatile Random Access Memory

O**OA&M**

Operations, administration, and maintenance

object linking and embedding

A compound document standard that enables you to create objects with one application and then link or embed them in a second application.

OEM

Original equipment manufacturer

online/offline table

The online/offline table is configured on the RLC. It allows you to schedule times that the host PBX connection is made available to the remote site and at which times all telephones at the remote site can use only the local telephone service.

The online/offline table is used for controlling ISDN BRI costs.

Open System Interconnection

A worldwide communications standard that defines a framework for implementing protocols in seven layers.

OS

Operating Standard

OSI

Refer to Open System Interconnection.

OTM

Optivity Telephony Manager. This is a Nortel software application that is used to administer the Meridian 1 PBX.

P**Packet InterNet Groper**

PING. A protocol that can be used to test the Ethernet connection to devices on the network (such as the RLC and its associated remote units).

packetized voice

Digital Signal Processors (DSPs), located in the Remote Gateway 9150 unit and RLC, convert analog voice into digital data. The data is constructed as a UDP/IP voice packet for transmission over an IP network.

parity

The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communications to ensure the validity of data.

PBX

Refer to private branch exchange.

pegging

The action of incrementing statistical counters to track system events.

pegging threshold

A threshold used to define a cut-off value for statistics such as short call and service level. Pegging thresholds are used in reports and historical statistics.

personal directory number

A DN on which an agent can be reached directly, usually for private calls.

PING

Refer to Packet InterNet Groper.

POST

Refer to Power-On Self-Test.

Power-On Self-Test

Initializes and performs rudimentary tests on baseboard hardware, including CPU, floating point unit, interrupts, memory, real-time clock, video, and auto-initializing PCI and EISA bus.

priority DN

A user station can be configured as a priority DN. There are two levels of priority—high and normal. High priority level allows you to

- ensure a trunk is always available
- use PSTN trunking for the host PBX connections
- move the high priority DN first from the IP network to the PSTN

private branch exchange

A telephone switch, typically used by a business to service its internal telephone needs. A PBX usually offers more advanced features than are generally available on the public network. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

protocol

A standard format used for communication between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

PSTN

Public Switched Telephone Network (also known as the public telephone network).

Q**Quality of Service (QoS) Transitioning Technology**

Technology that automatically switches calls from the IP network to the PSTN when the voice QoS falls below a predetermined threshold, and back to the IP network when the QoS returns to normal.

R

RAM

Random Access Memory. This is the most common type of memory found in computers and other devices, such as printers. The term RAM is usually synonymous with main memory, the memory available to programs. For example, a computer with 8 Mbytes of RAM has approximately 8 million bytes of memory that programs can use.

remote station

A telephone set or fax machine located at the Remote Gateway 9150 site.

remote trunk

From the RLC's point of view, remote trunks are the ISDN BRI connections between the PSTN and the Remote Gateway 9150 unit located at the branch office site.

RJ-45 connector

An 8-position, 8-conductor modular jack that provides the 10BaseT Ethernet connection.

ROM

Read-Only Memory. This is the computer memory on which data has been prerecorded and from which it cannot be removed.

router

A device that connects two LANs. Routers are similar to bridges but provide additional functionality, such as the ability to filter messages and forward them to different places based on various criteria.

S

second-level threshold

The value used in display thresholds that represents the highest value of the normal range for a given statistic.

security identifier

The remote unit sends the branch office security identifier (password) to the RLC for each connection request. The RLC matches the identifier configured for the RLC port. When it finds a match, it grants access to the port and allows the call to proceed.

serial port

A general-purpose interface that can be used for almost any type of device, including modems, mice, and printers (although most printers are connected to a parallel port). Most serial ports on personal computers conform to the RS-232C or RS-422 standards.

server

A computer or device on a network that manages network resources. Examples of servers include file servers, print servers, network servers, and database servers.

service

A process that adheres to a Windows NT structure and requirements. A service provides system functionality.

Service Control Manager

A Windows NT process that manages the different services on the PC.

silence suppression

A feature that prevents packet transmission during periods when there is no voice data present.

Simple Network Management Protocol

A set of protocols for managing complex networks. SNMP sends messages called protocol data units (PDUs) to different parts of a network, and then analyzes the responses.

single-user ports

A RLC port that supports one remote station.

SNMP

Refer to Simple Network Management Protocol.

SPID

Service Profile Identifier

SPRE code

A Special Prefix code that is used to initiate use of a PBX feature. In a Remote Gateway 9100 Series context, SPRE codes are used to

- toggle a remote site between online and offline modes
- use the paging feature
- switch an analog or ATA-equipped station from host-controlled mode to locally controlled mode so that local calls can be made
- register a Remote Gateway 9150 unit for a multi-user or dynamic port

station

A telephone or fax machine located at a Remote Gateway 9150 site.

stop bit

In asynchronous communications, a bit that indicates a byte has just been transmitted. Every byte of data is preceded by a start bit and followed by a stop bit.

subnet mask

A subnet mask is the part of the IP address used to represent a subnetwork within a network. A typical IP address might be 192.210.34.144. Each part of this address is made up of eight bits. The subnet mask identifies to the RLC or remote unit what portion of the IP address represents the network (and subnetwork) and what portion represents the host.

switch

In a telecommunications network, a switch is the hardware that receives phone calls and provides connections to telephone sets. The switch allows a connection to be established as necessary and terminated when there is no longer a session to support it.

In data networks, a switch is a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) of the OSI Reference Model and, therefore, support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

switch resource

A device that is configured on the switch.

T**TCP/IP**

Transport Control Protocol/Internet Protocol. The communication protocol used to connect devices on the Internet. TCP/IP is the standard for transmitting data over networks.

threshold

A value for a statistic at which system handling of the statistic changes.

threshold class

A set of options that specifies how statistics are treated in reports and real-time displays. *Refer also to* pegging threshold.

trunk

A communications link between a PBX and the public central office, or between PBXs. Various trunk types provide services such as Direct Inward Dialing (DID), ISDN, and central office connectivity.

trunk access code

A trunk access code is a number that is used by the Remote Gateway 9150 unit to determine which trunk to use when routing a call. For example, 9 is a common trunk access code used to obtain an outside line.

Note: All trunk access codes are configured on the Remote Gateway 9150 unit with a pound sign (# in North America) so that there are no conflicts with host PBX numbering plans.

trunk groups

A trunk group consists of one or more trunk lines that are logically grouped. You can configure up to eight trunk groups on the Remote Gateway 9150 unit.

trunk interface modules

Used to route calls over the PSTN. The number of modules you must install on the Remote Gateway 9150 unit depends on the number of simultaneous calls you want in host-controlled or locally controlled mode.

U

Uninterruptible Power Supply

A power supply that includes a battery to maintain power in the event of a power outage. Typically, a UPS keeps a computer running for several minutes after a power outage, enabling you to save data that is in RAM and to shut down the computer safely.

UPS

Refer to Uninterruptible Power Supply.

utility

A program that performs a specific task, usually related to managing system resources. Operating systems contain a number of utilities for managing disk drives, printers, and other devices.

V

voice compression

Prior to transmission, the voice data is compressed; after transmission, the data is converted back to voice data at the destination. Voice compression means that voice consumes less bandwidth, leaving more bandwidth for data or other voice or fax communications.

voice jitter attenuation

A feature that removes the variable delays from the voice packets sent across the IP network, thus avoiding awkward-sounding speech.

Voice over IP (VoIP)

Technology that uses the IP data network to carry the voice conversation and telephone set control signals between a remote site and the host PBX.

W

WAN

Wide area network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs). The largest WAN in existence is the Internet.

Fields index

Symbols

%Error 330

Numerics

802.1Q Mapping 195
Priority 195
VLAN ID 195

A

Add on Module Type 210
Admin 313
Auto Hold 210, 223
Available Channels 309, 317
Available Flex Channels 309
Available MIPS 309
Available Modem Channels 309

B

B Channel 238
B Channel Usage 125
Bandwidth (BW) Connection Statistics
 IP QoS Status 299
 No of Voice Calls on IP 299
 No of Voice Calls on PSTN 299
 Remote Unit Number 299
 Signaling Status 299
 Total Up Trunk BW 299
 Used IP BW 299
 Used Trunk BW 299

Bandwidth Connection Statistics
 field descriptions 299
Block Incoming Local Call on Primary B Channel 204
BRI Information Statistics
 Available Channels 317
 Cross Connection Type 317
 Device Number 317
 In Service 317
 Module Index 317
 Module Number 317
 Name 317
 Total Channels 317
 Usage 317
Bridge Port 211, 223
Browse
 Upload Configuration 287
Browse (button)
 Software Upload 341

C

Call BW 302
Call Duration 319
Call Start Time 319, 321
Call Status 324
Call Type 296
Called Number 296
Caller ID 201
Caller Info Statistics
 Call BW 302
 Connection ID 302
 Current Media 302
 Last Transition to IP 302
 Last Transition to PSTN 302

- Priority 302
- Remote ID 302
- Start Time 302
- Transitions to IP 302
- Transitions to PSTN 302
- Type 302
- Channel 313
- Close Time 296
- Collisions 331
- COM port number 164
- Compression Algorithms 242
- Connection ID 302, 321
- CPND 210
- Cross Connection Type 317
- Current Media 302

D

- Date
 - Auto Upgrade 246
- Day
 - Auto Upgrade 245
- Default (button) 143
- Delete
 - Syslog Configuration 249
- Device 238
- Device Information Statistics
 - Call Status 324
 - Device Type 324
 - Login Status 324
 - ROU Port Number 324
 - Type 324
- Device Number 309, 317
- Device Type 324
- DiffServ CodePoint 194
 - Value 194
- DN 210, 223
- DSP Load 241
- DSP Statistics
 - Name 310

- DSP statistics
 - Available Channels 309
 - Available Flex Channels 309
 - Available MIPS 309
 - Available Modem Channels 309
 - Device Number 309
 - In Service 309
 - Module Number 309
 - Single Dig Dev ID 309
 - Total Channels 309
 - Total Flex Channels 309
 - Total MIPS 309
 - Total Modem Channels 309
 - Total Reserved Channels 310
 - Total Tones Channels 310
 - Total Voice Channels 309
- Duration 296, 321

E

- Emergency Feature 180
- Enable PBX Alarms 181
- Enter a node name to recognize the unit 121
- Enter the local IP Address of the unit 121
- Enter the Local IP Gateway of the unit 121
- Enter the Local IP Mask of the unit 121
- Enter the PSTN Number 125
- Enter the SPID Number 125
- Ethernet Interface Statistics
 - Admin 313
 - Channel 313
 - IFC No 313
 - IFC Type 313
 - LAN Drv 313
 - MTU Len 313
 - Oper 313
 - Speed 313
- EthRx Disc 331
- EthRx Err 331
- EthRx Mcast 330

EthRx Ucast 331
EthTx Disc 330
EthTx Err 331
EthTx Mcast 330
EthTx Ucast 330

F

Facility Indicator 249
Forward Busy/No Answer 211, 223
 Number of Rings before transfer 211
 Transfer to DN 212
Frequency 245
Full Duplex Ethernet 196

G

Group No 237

H

Hardware Statistics
 Module No 306
 Module Type 306
 Status 306
 Version 306
Help (button) 143
Hour 329

I

IFC No 313
IFC Type 313
In Service 309, 317
International Tones 185
 Cadence Time 190
 End Repeat 189
 No of Cycles 190
 Tone Code 189
 Tone Type 189

IP Address 161, 193
 RLC Connection Configuration 203
 Software Upload 341
 Syslog Configuration 249
 Upload Configuration 286
IP Connection 203
IP Gateway 193
IP Network Mask 193
IP QoS Status 299
IP Signaling 204
ISDN Line Type 229
ISDN Module Information
 Link Status 326
 Module Number 326
 Module Type 326
 Usage 326

L

LAN Drv 313
Last Transition to IP 302
Last Transition to PSTN 302
Link Status 326
Local Call Keys 212, 223
Local Call Statistics
 Call Duration 319
 Call Start Time 319
 Port No. 319
Local CPND 223
Local DNs to Alert 237
Local SwitchOver 184
Login Status 324

M

Module
 Software Upload 340
 Trunk Group B-Channel 238
Module # 228
Module Index 317
Module No 306

Module Number 241, 309, 317, 326
Module Status 124
Module Type 306, 326
MTU Len 313
Multiple Subscriber Number 185

N

Name 310, 317
Network Statistics
 %Error 330
 Collisions 331
 EthRx Disc 331
 EthRx Err 331
 EthRx Mcast 330
 EthRx Ucast 331
 EthTx Disc 330
 EthTx Err 331
 EthTx Mcast 330
 EthTx Ucast 330
 Hour 329
 Rx Dropped 329
 Rx Error 329
 Rx Voice Samples 329
 Tx Voice Samples 329
No of Voice Calls on IP 299
No of Voice Calls on PSTN 299
Node Name 178
Number of Devices 241

O

OK (button) 143, 148, 153
Oper 313
Optional Feature Keys 213

P

Paging 210, 223
Phone Type 210
Port No. 319

Port Type 208, 222
Priority 302
Provision ID 202
PSTN Connection 203
PSTN Number 231

R

Remote Call Statistics
 Call Start Time 321
 Connection ID 321
 Duration 321
 RLC ID 321
 RLC Port No. 321
 ROU (Remote Gateway 9150 unit) Port No. 321
Remote ID 296, 302
Remote Unit Number 299
Retrieve (button) 143, 150, 153
RLC ID 321
RLC Port 208, 222
RLC Port No. 321
ROU (Remote Gateway 9150 unit) Port No. 321
ROU Port Number 324
Rx Dropped 329
Rx Error 329
Rx Voice Samples 329

S

Security Level 201
Select the Country Type 125
Select the Protocol Type 125
Send (button) 143, 149, 153
Set the unique Unit ID of the unit 120
Set the Unit ID of the RLC to connect to 122
Signaling Status 299
Single Dig Dev ID 309
Speed (statistic) 313
SPID 231

SPRE Codes

DeRegistration 182

Local Calling 182

Offline 182

Online 181

Paging 181

Registration 182

Start Auto Upgrade 245

Start Time 296, 302

statistics

Bandwidth (BW) Connection Statistics

IP QoS Status 299

No of Voice Calls on IP 299

No of Voice Calls on PSTN 299

Remote Unit Number 299

Signaling Status 299

Total Up Trunk BW 299

Used IP BW 299

Used Trunk BW 299

Bandwidth Connection Statistics

field descriptions 299

BRI Information Statistics

Available Channels 317

Cross Connection Type 317

Device Number 317

In Service 317

Module Index 317

Module Number 317

Name 317

Total Channels 317

Usage 317

Caller Info Statistics

Call BW 302

Connection ID 302

Current Media 302

Last Transition to IP 302

Last Transition to PSTN 302

Priority 302

Remote ID 302

Start Time 302

Transitions to IP 302

Transitions to PSTN 302

Type 302

Caller Info Statistics field descriptions 302

Device Information Statistics

Call Status 324

Device Type 324

Login Status 324

ROU Port Number 324

Type 324

DSP Statistics

Name 310

DSP statistics

Available Channels 309

Available Flex Channels 309

Available MIPS 309

Available Modem Channels 309

Device Number 309

In Service 309

Module Number 309

Single Dig Dev ID 309

Total Channels 309

Total Flex Channels 309

Total MIPS 309

Total Modem Channels 309

Total Reserved Channels 310

Total Tones Channels 310

Total Voice Channels 309

Ethernet Interface Statistics

Admin 313

Channel 313

IFC No 313

IFC Type 313

LAN Drv 313

MTU Len 313

Oper 313

Speed 313

Hardware Statistics

Module No 306

Module Type 306

Status 306

Version 306

ISDN Module Information

- Link Status 326
- Module Number 326
- Module Type 326
- Usage 326

Local Call Statistics

- Call Duration 319
- Call Start Time 319
- Port No. 319

Network Statistics

- %Error 330
- Collisions 331
- EthRx Disc 331
- EthRx Err 331
- EthRx Mcast 330
- EthRx Ucast 331
- EthTx Disc 330
- EthTx Err 331
- EthTx Mcast 330
- EthTx Ucast 330
- Hour 329
- Rx Dropped 329
- Rx Error 329
- Rx Voice Samples 329
- Tx Voice Samples 329

Remote Call Statistics

- Call Start Time 321
- Connection ID 321
- Duration 321
- RLC ID 321
- RLC Port No. 321
- ROU (Remote Gateway 9150 unit) Port No. 321

Trunk Connection Statistics

- Call Type 296
- Called Number 296
- Close Time 296
- Duration 296
- Remote ID 296
- Start Time 296
- Status 296
- Trunk Number 296

- Trunk Connection Statistics field descriptions 296

- Status 296, 306

- Auto Upgrade Configuration 245

- BRI Configuration 230

- Syslog Configuration 249

- Trunk Group Configuration 237

- Switch Type 230

T

TFTP Server

- IP Address 245

Time

- Auto Upgrade 245

- Time Offset 179

- Total Channels 309, 317

- Total Flex Channels 309

- Total MIPS 309

- Total Modem Channels 309

- Total Reserved Channels 310

- Total Tones Channels 310

- Total Up Trunk BW 299

- Total Voice Channels 309

- Transitions to IP 302

- Transitions to PSTN 302

- Trunk Access Code 237

Trunk Connection Statistics

- Call Type 296

- Called Number 296

- Close Time 296

- Duration 296

- field descriptions 296

- Remote ID 296

- Start Time 296

- Status 296

- Trunk Number 296

- Trunk Group B Channels 238

- Trunk Group B-Channel dialog box 238

- Trunk Number 296

- Trunk Support 183

Tx Voice Samples 329
Type 230, 302, 324

U

Unit ID
 9150 System Configuration 178
 RLC Connection Configuration 203
Usage 317, 326
Used IP BW 299
Used Trunk BW 299

V

Version 306

W

Which module would you wish to configure 124
Wish to configure Multiple 9150 Ports 123
Wish to Enable IP Voice Connection to Remote
 122
Wish to Enable PSTN Connection to RLC 123

Index

Numerics

- 10BaseT Ethernet 10
 - as a component xix
 - connection option 10
- 10BaseT Ethernet connection xix
- 25-pair connector 5
- 802.1Q Mapping 34
- 9150
 - configuration
 - Auto Upgrade 244
 - Syslog 248
- 9150 Port Configuration
 - Bridge Ports 214
 - configuration scenarios 215, 216, 217, 218, 219
- 9150 Port Configuration property sheet 207
- 9150 System Configuration
 - NLP 175

A

- ACD
 - Local Calling key 32
 - M3905 digital telephone set 27
 - Make Set Busy mode 32
 - Not Ready mode 32
 - Remote Connection Configuration property sheet (RLC) 32
 - RLC Port Configuration property sheet 32
 - User On Demand Idle Timer 32
 - User On Demand Minimum Call Timer 32
- ACD agent 32
- ACD applications 32
 - refer to* Automatic Call Distribution applications
- add-on modules 30
 - DSP application modules 9
 - trunk interface modules 8
- Admin connector pin-out table 409
- administration
 - password
 - changing 280, 281
 - password, changing 280
 - PC
 - connection options 59
 - Optivity Telephony Manager and Configuration Manager 63
 - software
 - command line interface 44
 - Configuration Manager 43
 - connection options 43
- Alarms and alerts 366
 - display logs 412
- analog calling
 - required configuration 220
- analog port 11, 220
 - basic POTS functionality 220
 - configuring 222
 - functionality not provided 220
- Analog Telephone Adapters 30
- application modules 30
- associating trunk groups with local stations 254
- ATA 257
 - maximum quantity 257
 - refer to* Analog Telephone Adapters
- ATA equipped stations 257
- Auto Answer Back
 - M26xx digital telephone sets 26
- Auto Hold 274
- auto logoff 158
- Auto Upgrade
 - Auto Upgrade Configuration property sheet 243, 342
- Auto Upgrade configuration
 - procedure 244
- Automatic Call Distribution
 - refer to* ACD
- Automatic TEIs
 - multi-point configuration 227
 - point-to-point configuration 227

B

- B Channel
 - Trunk Group B-Channel 238
- backup
 - configuration file, creating 282
- bandwidth
 - allocating 65
 - allocation, description 14
 - approximate total 42
 - extra 37
 - measuring
 - Bandwidth Connection Statistics 297
 - peak
 - according to Codec 42
 - priority reserved 37
- Bandwidth Connection statistics 297
- Bandwidth Connection Statistics screen 297
 - descriptions 299
 - displaying 298
- Boot status
 - LED indicator 4
- BRI
 - Automatic TEIs
 - multi-point configuration 227
 - point-to-point configuration 227
 - refer also to* Basic Rate Interface
- BRI Configuration property sheet 225
- BRI trunks
 - configuring 225
 - Norway and Sweden 226
- Bridge Port 211
 - configuration
 - requirements 211, 250, 251
 - releasing 214
- Bridge Ports 214, 250
 - configuration scenarios 215, 216, 217, 218, 219

C

- calculating dial tone delay 254
- Call appearance keys
 - MADN 253
 - SCR/SCN keys 253

- call appearance keys 253
 - defined 253
 - dial tone delay 253, 254
 - host call appearance key 261
 - local call appearance key 262
- call blocking 57
 - calculating system requirements 58
 - defined 57
 - reducing between Remote Gateway 9150 unit and host PBX 58
- Call Forward 211, 276
- Call Log
 - M39xx digital telephone sets
 - country code 27
 - trunk access code 27
- call set-up duration 254
 - ISDN line set-up 254
- Call Transfer 275
- call transfer
 - trunk-to-trunk 275
- Call Waiting 274
- caller identification (security level) 12
- Caller Information Statistics screen 300
 - displaying 301
- calling permissions and restrictions 255
- calls
 - emergency service 273
 - host-controlled calls 265
 - methods for placing outgoing calls 265
 - outgoing locally controlled calls 266
 - placing 264
 - receiving 264
 - station-to-station calls 267
- Channel Number 334
- circuit only priority 36
- clearing logs 293
- Codecs
 - supported 42
 - data stream 42
 - G.711 42
 - G.726 42
 - G.729A 42
- coding law
 - ISDN line type 226
- Collisions 314
- collisions 5

- communications system and software
 - requirements 42
- communications system requirements 42
- Companding Algorithm
 - configuring 185
 - ISDN line type 226
- components
 - 10BaseT Ethernet connection xix
 - Digital Signal Processor (DSP) xix
 - ISDN Basic Rate Interface connection xix
 - ISDN BRI trunk interface modules xix
 - Remote Gateway 9150 unit xix
- compression algorithms 67
 - and ATA devices 257
 - and MCA devices 257
 - G.711 257
 - G.729A 257
 - G.729A/FAX 257
 - no compression 257
- Computer Telephony Integration applications 31
- Conference calling 276
- configuration
 - Auto Upgrade 244
 - Auto Upgrade Configuration property sheet 243, 342
 - backup
 - creating 282
 - Bridge Port
 - requirements 211, 250, 251
 - Bridge Ports 215, 216, 217, 218, 219
 - DSP Configuration property sheet 239
 - EAC 176
 - host PBX 222
 - MCA 75
 - IP
 - addresses 193
 - IP addresses
 - saving to Flash 193
 - IP configuration
 - Full Duplex Ethernet 196
 - MADN 253
 - MCAs and ATAs
 - maximum quantity 257
 - Phone Type 207
 - recommendation 390
 - Remote Gateway 9100 Series unit
 - connection types 134
 - Remote Gateway 9150 unit
 - Companding Algorithm 185
 - defining a fax station 221
 - NLP 175
 - RLC
 - connection types 134
 - samples
 - Meridian 1 PBX data port 394
 - Meridian 1 PBX voice port 392
 - Remote Gateway 9150 400
 - RLC 396
 - Syslog 248
 - Syslog Configuration property sheet 247
- Configuration Manager
 - check boxes 140
 - command buttons 143
 - configuration
 - downloading 155
 - uploading 155
 - configuration file
 - creating 154
 - opening 154
 - description 134
 - device type, selecting 156
 - ending a session 171
 - file operations
 - description 148
 - diagram 145
 - logging on to a unit 157
 - menus 137
 - option buttons 140
 - parts of the screen 137
 - password 280
 - property sheets 139
 - scroll boxes 141
 - shutdown
 - performing 169
 - system restart
 - performing 169
 - system tree 138
- Configuration Wizard
 - how it works 115
 - introduction 115
 - starting 116

- configuring
 - key labels
 - M3902 digital telephone sets
 - Local keys 27
 - Remote Gateway 9150 unit
 - BRI trunks 225
 - Norway and Sweden 226
 - configuring Remote Gateway 9150 unit
 - 9150 Port Configuration sheet 207
 - BRI Configuration sheet 225
 - Cadence Time 190
 - emergency number 180
 - End Repeat 189
 - International Tones 186
 - local switchover 184
 - Multiple Subscriber Number 185
 - No of cycles 190
 - RLC Connection Configuration sheet 198
 - RLC connection information 198
 - security level 200
 - SPRE codes, defining 181–182
 - system identification information 178
 - Tone Code 189
 - Tone type 189
 - Trunk Group Configuration sheet 232
 - trunk groups, configuring 232
- connecting the Remote Gateway 9150 unit
 - cables you must provide 105
 - connection panel diagram 107
 - pin-out references 106
- connection
 - what to do if the PING did not work 364
- connection bandwidth
 - extra bandwidth 37
 - priority reserved bandwidth 37
- connection options
 - 10BaseT Ethernet interface 10
 - analog port for fax machines 11
 - ethernet connection 60
 - ISDN BRI lines to PSTN 10
 - QoS Transitioning Technology 10
 - serial connection 59
- connection types 14
- connectivity
 - troubleshooting
 - PING failure 364
- connector pin-out tables
 - Admin 409
 - Ethernet 408
 - Power 410
 - Telco 1 404
 - Telco 2 406
- connectors
 - 25-pair 5
 - DB-9 6
 - RJ-45 5
- country code
 - M39xx digital telephone sets 27
- cover, removing the Remote Gateway 9150 90
- CRC Errors 334
- creating private lines 255
- CS 1000 xxiv
- CS 2100 xxiv
- CTI applications
 - refer to* Computer Telephony Integration applications
- ## D
- data stream 42
 - DB-9 connector 6
 - default algorithm 33
 - defining a fax station 221
 - deploying Remote Gateway 9150 unit
 - overview 75
 - port and station assignment 75
 - Voice over IP mode, implementing 77
 - deployment
 - Remote Gateway 9150 unit
 - QoS Transitioning Technology 79
 - Device
 - Trunk Group B-Channel 238
 - device connectivity 356
 - Device Information screen 322
 - dial tone
 - analog port 220
 - dial tone delay 253, 254
 - calculating 254
 - call set-up duration 254
 - ISDN line set-up 254
 - Remote Gateway 9100 Series 254

- Differentiated Services (DiffServ) 34
- Digital Signal Processor (DSP) *xix*
- digital telephone sets
 - supported
 - M39xx series accessories 30
 - supported models 26
 - M2006 26
 - M2008D 26
 - M2008HFD 26
 - M2216D 26
 - M2616D 26
 - M3110 26
 - M3310 26
 - M3820 26
 - M3901 26
 - M3902 26
 - M3903 26
 - M3904 26
 - M3905 26
- digital telephones
 - display messages 270
 - supported 26
 - troubleshooting 351
- Disabled Outbound Digit Sequence 212
- display messages 270
- displaying logs 290
- download
 - M3904 digital telephone sets
 - Flash upgrade 28
- Download Configuration 152, 153
- DSP
 - calculating system requirements 385
 - compression algorithms
 - G.711 257
 - G.729A 257
 - G.729A/FAX 257
 - no compression 257
 - DSP Configuration property sheet 239
 - MCR keys 254
 - SCR/SCN keys 253
- DSP modules
 - adding 72
 - installing 96
 - removing 96
 - when to install 93
 - where they can be installed 94

- DSP Statistics 309
- DSP Statistics screen 307
- DTMF tones
 - analog port 220
- dynamic port pooling 35

E

- EAC
 - configuration 176
- emergency
 - activation code
 - description of 41
 - calls, placing 273
 - service calls 273
 - service number 180
- Emergency Access Code
 - refer to* EAC
- Emergency service programmability 176
- EPROM checksum validation 111
- equipment
 - supported applications
 - Automatic Call Distribution applications 32
 - Computer Telephony Integration applications 31
 - supported digital telephone sets 26
 - M2006 26
 - M2008D 26
 - M2008HFD 26
 - M2216D 26
 - M2616D 26
 - M3110 26
 - M3310 26
 - M3820 26
 - M3901 26
 - M3902 26
 - M3903 26
 - M3904 26
 - M3905 26
 - supported telephone modules 30
 - add-on modules 30
 - Analog Telephone Adapters 30
 - application modules 30
 - Meridian Communication Adapters 30

- Ethernet
 - collisions 5
 - connector pin-out table 408
 - LED indicator 4
- Ethernet connection
 - default 10
 - full-duplex 10
 - half-duplex 10
- Ethernet Interface Statistics
 - Collisions 314
 - QLen 314
 - Rx Disc 314
 - Rx Err 314
 - Rx Mcast 313
 - Rx Octet 313
 - Rx Ucast 313
 - Tx Disc 314
 - Tx Err 314
 - Tx Mcast 314
 - Tx Octet 314
 - Tx Ucast 314
- extra bandwidth 37

F

- fax
 - host PBX configuration 222
- fax port, configuring 222
- fax support 41
- features
 - supported 39
 - supported with Bridge Ports 39
 - Voice over IP
 - packet loss handling techniques 33
 - packetized voice 33
 - silence suppression 33
 - voice jitter attenuation buffer 33
- field descriptions
 - Local Profile Configuration 211
- File Open 148, 153
- File Save As 149, 153
- Firewall device 167

- firmware
 - types of 337
 - upgrade
 - performing 338
 - upgrade files
 - downloading 337
 - version, verifying 335
- flash checksum validation 111
- Flash download
 - M39xx digital telephone sets 338
- Flash upgrade
 - M39xx digital telephone sets
 - download time 28
- Frame Length Violations 334
- full-duplex Ethernet 10, 196
- future growth
 - DSP modules, adding 72
 - maximum configurations 73
 - trunk interface modules, adding 73

G

- G.711 33, 42, 257
 - approximate total bandwidth 42
 - data stream 42
- G.726 33, 42
 - approximate total bandwidth 42
- G.729A 33, 42, 257
 - approximate total bandwidth 42
- G.729A/FAX 257
- general safety
 - introduction 86
 - precautionary messages 86
 - safety precautions 87
- GUI
 - Auto Upgrade Configuration property sheet
 - 243, 342
 - DSP Configuration property sheet 239
 - Syslog Configuration property sheet 247

H

- half-duplex Ethernet 10
- hardware description
 - connectors 5
 - LED indicators 4
 - mounting options 6
 - Remote Gateway 9150 unit
 - LED indicators 3
- hardware installation tools 88
- Hardware Statistics 303
- host-controlled mode 260
 - and Call Transfer feature 275
 - and Call Waiting feature 274
 - and Hold feature 274
 - calls, placing 265
 - external corporate call, example 22
 - indicator updates 268
 - internal corporate call, example 20

I

- idle timer 15
- implementation
 - QoS Transitioning Technology 79
- incoming call process 17
- incoming calls
 - receiving 264
- indicators, telephone
 - host-controlled indicator updates 268
 - introduction 268
 - locally controlled indicator updates 269
- installation 98
 - Remote Gateway 9150 unit 98
- installing the Remote Gateway 9150 unit 98
 - Configuration Wizard 115
 - connecting 105
 - cover, removing 90
 - general safety 86
 - mounting 98
 - network connections, testing 129
 - powering up 111
 - software, installing 113
 - unpacking and inspecting 89
- installing, planning for
 - telecom manager's installation checklist 46
- interface loopbacks 111

- International Tones 186
- Internet Protocol
 - refer to* IP
- IP
 - addresses 83
 - addressing and routing 55
 - configuration
 - addresses 193
 - saving to Flash 193
 - interface, configuring 192
- IP Configuration property sheet 192
- IP only priority 36
- ISDN Basic Rate Interface connection xix
- ISDN BRI
 - BRI Configuration sheet 225
 - connection option 10
 - planning for 82
 - trunks groups, configuring 232
 - trunks, configuring 225
- ISDN line set-up 254
- ISDN Line Type
 - default coding law 226
- ITE Frame Length Violations 334
- ITE Receive Busy Errors 334
- ITE Transmitter Underruns 334

K

- Key Feature Configuration dialog box 213
- key map
 - M3904 digital telephone set 27

L

- LED indicators
 - Boot status 4
 - Ethernet 4
 - hardware description 4
 - Module 4
 - Power 4
 - power up behavior 111
 - troubleshooting 349
 - V.35 4
- local call appearance keys 253, 254
 - call set-up duration 254
 - ISDN line set-up 254

- local calling
 - Bridge Port 39
 - call restrictions 39
 - digital telephone features
 - supported 39
 - supported with Bridge Ports 39
 - local calls through PSTN 39
 - local extension calling 38
 - multiple DN appearances 261
 - Local Calling key 32
 - Local keys
 - M3902 digital telephone sets
 - key labels 27
 - Local Profile Configuration
 - field descriptions 211
 - Local Profile Configuration dialog box 209, 223
 - local ringback
 - analog port 220
 - local stations
 - trunk groups 254
 - local switchover 184
 - local trunk calls
 - pre-dialing 261
 - locally controlled mode 18, 261
 - Call Transfer feature 275
 - Call Waiting feature 274, 275
 - calls, placing 266
 - Hold feature 274
 - indicator updates 269
 - local call, example 24
 - local trunk calls
 - pre-dialing 261
 - logging off from a unit
 - auto logoff 158
 - logging off of a unit 166
 - logging on to a unit
 - connection history 157, 158
 - connection types 157
 - default logon ID and password 157
 - from Configuration Manager 157
 - logging on to multiple Remote Gateway 9100
 - Series units 167
 - logon ID
 - Configuration Manager 280
 - RLC 280
 - unit 157
 - logs
 - clearing 293
 - resizing 292
- ## M
- M2006 26
 - M2008D 26
 - M2008HFD 26
 - M2216D 26
 - M2616D 26
 - M26xx digital telephone sets
 - Auto Answer Back 26
 - CS 2100
 - Auto Answer Back 26
 - M3110 26
 - M3310 26
 - M3820 26
 - M3901 26
 - M3902 26
 - M3902 digital telephone sets
 - Local keys
 - key labels 27
 - M3903 26
 - M3904 26
 - M3904 digital telephone set
 - key map
 - Virtual Office 27
 - M3904 digital telephone sets
 - firmware
 - download 27
 - upload 27
 - M3905 26
 - M3905 digital telephone set
 - ACD queue
 - log on 27

- M3905 digital telephone sets
 - firmware
 - download 27
 - upload 27
 - Phase I
 - Remote Gateway 9150 unit reboot 27
- M39xx digital telephone sets
 - Flash download
 - download time 338
 - Flash upgrade
 - download time 28
 - PBX downgrade 28
 - software upgrade
 - download time 338
- M39xx digital telephone sets
 - Call Log
 - country code 27
 - trunk access code 27
- MADN 253
 - dial tone delay
 - calculating 254
- Make Set Busy (MSB) mode
 - ACD 32
- maximum collision re-try counter 5
- MCA 257
 - maximum quantity 257
 - refer to Meridian Communication Adapters*
- MCA equipped stations 257
- MCR keys
 - DSP requirements 254
- Meridian 1 PBX xxiv
 - data port configuration (example) 394
 - voice port configuration (example) 392
- Meridian Administration Tools (MAT) 63
- Meridian Communication Adapters 30
- messages, telephone display 270
- minimum call duration timer 14
- Module
 - LED indicator 4
 - Trunk Group B-Channel 238
- mounting the Remote Gateway 9150 unit
 - choosing a suitable location 98
 - installing in a rack 103
 - installing on a desk 99
 - installing the unit on the wall 100
- MSN 185

- Multiple Appearance Directory Number
 - refer to* MADN
- Multiple Call Ringing
 - refer to* MCR 254
- multiple DN appearances
 - local calling 261
- Multiple Subscriber Number
 - enabling 185
- multi-user ports 35

N

- NAPT routers 78
- NAT router 167
- NAT routers 78, 79
 - special configuration 79
- network
 - connecting the Remote Gateway 9150 unit
 - 109
 - considerations
 - call blocking 57
 - IP addressing and routing 55
 - network diagram 56
 - numbering plans 57
 - QoS 56
 - diagram (example) 391
 - testing
 - PSTN 131
 - no compression 257
 - no security (security level) 12
 - non-linear processor 175
 - normal priority 36
 - Norway and Sweden
 - BRI configuration
 - supplementary insulation 226
- Not Ready mode
 - ACD 32

O

- offline mode
 - defined 262
 - importance of 262
 - what controls offline mode 263
- OK 148, 153

- online help 144
- online mode
 - defined 262
 - what controls online mode 263
- online/offline
 - automatic offline event, overriding 278
 - scheduling 64
 - SPRE codes, using 277
- online/offline mode 262
 - changing 65
- online/offline table
 - configuration 40
 - description 40
 - how the table works 40
- optional modules
 - DSP application module 9
 - trunk interface module 9
- outgoing calls
 - placing 17, 264

P

- packet loss handling techniques 33
- packetized voice
 - default algorithm 33
 - G.711 33
 - G.726 33
 - G.729A 33
 - packet loss handling techniques 33
 - silence suppression 33
 - voice jitter attenuation buffer 33
- Paging 276
- password
 - Configuration Manager
 - changing 280
 - overview 280
 - local
 - changing 280
 - node
 - changing 281
 - Remote Gateway 9150 unit
 - changing 281
 - RLC 280
- password (for a unit) 157
- PBX
 - CS 1000 xxiv
 - CS 2100 xxiv
 - Meridian 1 PBX xxiv
- PBX downgrade
 - M39xx digital telephone sets 28
- PBX message
 - idle
 - updating 26
- PC
 - connection options 59
 - Optivity Telephony Manager and Configuration Manager 63
 - Windows PC requirements 62
- Phone Type 207
- physical environment 50
 - cables not included 53
 - connections 52
 - included cables 53
 - mounting options 52
- PING
 - failure 364
 - performing 362
 - unsuccessful PING 364
- placing calls 264
- planning
 - configuration 81
 - data entry forms
 - completion sequence 81
 - deployment options 75
 - future growth 72
 - network considerations 55
 - numbering plan 84
 - online/offline schedule 83
 - physical environment 50
 - security 70
 - station configuration 66
 - trunk configuration 84
 - trunk connection management 64
- port management
 - dynamic port pool 35
 - multi-user ports 35
 - single-user ports 35
- ports, types of 68

- POTS functionality
 - analog port 220
- Power
 - connector pin-out table 410
 - LED indicator 4
- power supply
 - cable 6
 - UPS compatibility 6
- power up
 - LED indicators 111
- precautionary messages 86
- pre-dialing
 - local trunk calls 261
- priority level
 - circuit only 36
 - IP only 36
 - normal 36
- priority reserved bandwidth 37
- private lines 255
- problems
 - solving
 - connectivity
 - PING failure 364
- Provision ID (security level) 12
- PSTN
 - testing 131
- PSTN mode
 - implementing 76
- PSTN Statistics
 - Channel Number 334
 - CRC Errors 334
 - Frame Length Violations 334
 - ITE Frame Length Violations 334
 - ITE Receive Busy Errors 334
 - ITE Transmitter Underruns 334
 - Receive Buffer Allocation Failures 334
 - Unknown Receive Errors 334
- PSTN testing 131

Q

- QLen 314
- QoS
 - network considerations 56
 - recovery 34

- QoS transition recovery 34
- QoS Transitioning Technology
 - connection option 10
 - connection options 10
 - implementation 79
 - log reports and statistics 35
 - Remote Gateway 9150 unit deployment 79
 - transport connections 34
 - trunk connections 64
- Quality of Service
 - refer to* QoS
- Quality of Service Transitioning Technology
 - refer to* QoS Transitioning Technology

R

- rack installation 103–104
- RAM memory test 111
- Reach Line Card
 - as a component xix
 - configuration (example) 396
- Receive Buffer Allocation Failures 334
- receiving calls 264
- releasing Bridge Ports 214
- Remote Call Statistics 320
- Remote Call Statistics screen
 - displaying 321
- Remote Connection command 167
- Remote Connection Configuration property sheet (RLC)
 - ACD 32
- Remote Gateway 9100 Series
 - dial tone delay 254
- Remote Gateway 9150
 - communications system requirements 42
 - software requirements 42
- Remote Gateway 9150 series
 - supported digital telephone sets
 - M39xx series accessories 30
- Remote Gateway 9150 unit 98
 - add-on modules 8
 - administering 279–346
 - analog port 220
 - as a component xix
 - ATA capacity 257

- cables you must obtain 105
 - configuration
 - defining a fax station 221
 - example 400
 - Configuration Wizard 115
 - connecting to the network 109
 - connection options 10
 - cover
 - removing 91
 - replacing 92
 - description 2, 3
 - Ethernet connection
 - default 10
 - full-duplex 10
 - half-duplex 10
 - how it works 16
 - implementation
 - NAPT routers 78
 - NAT routers 78, 79
 - LED indicators 3, 349
 - Boot status 4
 - Ethernet 4
 - Module 4
 - Power 4
 - power up behavior 111
 - troubleshooting 349
 - V.35 4
 - MCA capacity 257
 - mounting 98
 - network connections, testing 129
 - password
 - overview 280
 - password, changing 281
 - port management 35
 - powering up 111
 - software, installing 113
 - station priority and connection bandwidth 36
 - stations, using 259–278
 - troubleshooting 348
- Remote Gateway 9150 unit reboot
- M3905 digital telephone sets 27
- Remote Gateway 9150 units
- supported Codecs 42
- restarting the system
- when to perform a restart 169
- restore
- before you begin 285
 - upload a configuration file over the IP network 286
- Retrieve 150, 153
- ring trip voltage
- analog port 220
- RJ-45 connector 5
- RLC Connection Configuration property sheet
- 198
- RLC Port Configuration property sheet
- ACD 32
 - Rx Disc 314
 - Rx Err 314
 - Rx Mcast 313
 - Rx Octet 313
 - Rx Ucast 313
- ## S
- safety precautions 87
- Save to Flash 150
- SCR/SCN keys 253
- security
- data network security 70
 - description 70
 - identifier 12, 200
 - security level, configuring 200
 - system configuration 71
 - toll fraud 70
- Self-contained Firmware Upgrade 343
- Send 149, 153
- Send All 149, 153
- shutting down the system
- performing a system shutdown 170
 - when to perform a shutdown 169
- silence suppression 33
- single-user ports 35
- SLOTNO 304
- software
- installing 113
 - troubleshooting 360
 - upgrades
 - performing 346
 - version, verifying 335

- software requirements 42
- software upgrade
 - M39xx digital telephone sets 338
- SPRE codes
 - configuring 181–182
 - controlling online and offline modes 263
- Startup Information
 - SLOTNO 304
 - STATUS 304
 - TYPE 304
 - VERSION 304
- station configuration
 - call appearance keys 253
- stations
 - 9150 Device Configuration sheet 207
 - assignment and configuration 81
 - ATA and MCA-equipped stations and bandwidth requirements 257
 - call appearance keys 253
 - call processing capabilities and station settings 251
 - calling permissions and restrictions 255
 - configuration overview
 - Remote Gateway 9150 settings 68
 - RLC setting 66
 - Configuring Bridge Ports 250
 - defining 207
 - display messages 270
 - going online and offline 277
 - modes
 - controlling online and offline 263
 - host-controlled 260
 - importance of 262
 - locally controlled mode 261
 - of operation 260
 - offline mode 262
 - online mode 262
 - relationship between host-controlled and locally controlled modes 261
 - placing and receiving calls 264
 - priority
 - circuit only priority 36
 - IP only priority 36
 - normal priority 36
 - private lines 255
 - telephone features 273
 - telephone indicators 268
- station-to-station calls 267
- statistics
 - Bandwidth Connection Statistics screen 297
 - descriptions 299
 - displaying 298
 - Caller Information Statistics screen 300
 - displaying 301
 - Device Information screen 322
 - DSP Statistics screen 307, 309
 - Ethernet Interface Statistics
 - Collisions 314
 - QLen 314
 - Rx Disc 314
 - Rx Err 314
 - Rx Mcast 313
 - Rx Octet 313
 - Rx Ucast 313
 - Tx Disc 314
 - Tx Err 314
 - Tx Mcast 314
 - Tx Octet 314
 - Tx Ucast 314
 - Hardware Statistics screen 303
 - PSTN Statistics
 - Channel Number 334
 - CRC Errors 334
 - Frame Length Violations 334
 - ITE Frame Length Violations 334
 - ITE Receive Busy Errors 334
 - ITE Transmitter Underruns 334
 - Receive Buffer Allocation Failures 334
 - Unknown Receive Errors 334
 - Remote Call Statistics screen 320
 - displaying 321
 - Startup Information
 - SLOTNO 304
 - STATUS 304
 - TYPE 304
 - VERSION 304
 - Trunk Connection Statistics screen 294
 - description 296
 - displaying 295
 - STATUS 304

Status

refer also to Boot status

supported applications

ACD applications 32

Computer Telephony Integration applications
31

supported Codecs

data stream 42

G.711 42

G.726 42

supported CodecsG.729A 42**supported digital telephone sets 26**

M2006 26

M2008D 26

M2008HFD 26

M2216D 26

M2616D 26

M3110 26

M3310 26

M3820 26

M3901 26

M3902 26

M3903 26

M3904 26

M3905 26

M39xx series accessories 30

supported telephone modules 30

add-on modules 30

Analog Telephone Adapters 30

application modules 30

Meridian Communication Adapters 30

Syslog

Syslog Configuration property sheet 247

Syslog configuration

procedure 248

system

restart 169

shutdown 169, 170

System Configuration sheet 174**system security**

caller identification 12

no security 12

security identifier 12

system tree 138**T**

TEI 227

TEI Dropped 228

Telco 1

connector pin-out table 404

Telco 2

connector pin-out table 406

telephone features

Call Forward 276

Call Transfer 275

Call Waiting 274

Conference 276

emergency service calls 273

Hold 274

Paging 276

telephone modules

supported 30

add-on modules 30

Analog Telephone Adapters 30

application modules 30

Meridian Communication Adapters 30

telephones

digital telephones 26

refer also to stations

Terminal Endpoint Identifiers)

refer to TEI

tests

installation

what to do if tests do not work 130

PSTN 131

telephone connection

what to do if tests do not work 130

TFTP

firmware upgrades 338

server 62

tools required

hardware installation tools 88

software installation or upgrade tools 88

troubleshooting

before you begin 348

connectivity

PING failure 364

device connectivity 356

- digital telephone 351
- LED indicators 349
- overview 348
- Ping option 362
- recovering from a catastrophic failure 367
- Remote Gateway 9150 LED indicators 349
- software problems 360
- trunk access code
 - M39xx digital telephone sets 27
- trunk access codes 234
- Trunk Connection Statistics 294
 - descriptions 296
 - displaying 295
- trunk connections 13
 - bandwidth allocation 65
 - changing online/offline mode 65
 - managing 64
 - online/offline schedule 64
 - QoS Transitioning Technology 64
- Trunk Group B-Channel
 - fields
 - B Channel 238
 - Device 238
 - Module 238
- Trunk Group Configuration property sheet 232
- trunk groups 234
 - configuring 232
 - local stations 254
 - trunk access codes 234
- trunk groups, configuring 232
- trunk interface modules
 - adding 73
 - installing 96
 - removing 96
 - when to install 93
 - where they can be installed 94
- trunking
 - and idle timer 15
 - and minimum call duration timer 14
 - bandwidth allocation 14
 - connection types 14
 - types 13

- trunks
 - configuring 225
 - local and remote trunk 233
 - local trunk 233
 - managing trunk connections 64
 - remote trunk 233
 - trunk access codes 234
 - trunk groups 234
 - configuring 232
- trunk-to-trunk transfer 275
- Tx Disc 314
- Tx Err 314
- Tx Mcast 314
- Tx Octet 314
- Tx Ucast 314
- TYPE 304

U

- UDP port 20480
 - NAT configuration 79
- Unknown Receive Errors 334
- updating
 - PBX Idle message 26
- upgrades
 - performing
 - obtaining the latest upgrade file 337
 - software upgrade 346
- upgrades, performing
 - firmware upgrade 338
 - firmware version, verifying 335
 - software version, verifying 335
 - types of 337
 - upgrades and configuration files 339
 - when to perform 339
- Upload Configuration 151, 153
- UPS
 - requirements 6
- User On Demand Idle Timer
 - ACD 32
- User On Demand Minimum Call Timer
 - ACD 32

V

- V.35
 - LED indicator 4
- VERSION 304
- voice jitter attenuation buffer 33
- Voice over IP
 - implementing 77
 - packetized voice
 - default algorithm 33
 - G.711 33
 - G.726 33
 - G.729A 33
 - packet loss handling techniques 33
 - silence suppression 33
 - voice jitter attenuation buffer 33
- QoS Transitioning Technology 34

W

- wall mounting
 - installing 100–102

X

- X11 release 25.40
 - M39xx digital telephone sets 28

Remote Gateway 9150

Installation and Administration Guide

Copyright © 2005 Nortel. All Rights Reserved.

Printed in Canada.

All information contained in this document is subject to change without notice. Nortel reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

*Nortel, the Nortel logo, the Globemark, Unified Networks, Meridian 1 PBX, Communication Server 1000 (CS 1000), and Communication Server 2100 (CS 2100) are trademarks of Nortel.

TelStrat is a registered trademark of TelStrat International, Ltd. Microsoft, MS-DOS, and Windows are trademarks of Microsoft Corporation.

Publication number:	555-8421-215
Product release:	1.5
Document release:	Standard 3.1
Date:	January 2005

